UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA

Fatores Invariantes de Produtos e Somas de Matrizes

Paulo Alexandre Barbosa de Matos Firmino

Mestrado em Matemática

Dissertação orientada por:
Fernando Abel da Conceição Silva

2021

Agradecimentos

O meu sincero agradecimento ao Prof. Dr. Fernando Silva, orientador desta dissertação, pela sua inteira disponibilidade, por tudo o que me ensinou, e pelo seu apoio e constante motivação.

Agradeço a FCUL e o Departamento de Matemática e a todos os professores que contribuíram para a minha formação.

Obrigado!

Resumo

O conceito de fator invariante de uma matriz foi introduzido no séc. XIX por Smith. Segundo o seu teorema, qualquer matriz de números inteiros é equivalente a uma matriz diagonal, cujas entradas principais formam uma cadeia de divisibilidade, chamada forma normal de Smith. Foi depois generalizado para domínios de ideais principais comutativos. Notou-se também que o conceito se aplica a classes de anéis mais gerais.

Dados os fatores invariantes de duas matrizes, procurou-se determinar os possíveis fatores invariantes da sua soma e do seu produto. Introduzimos os resultados principais do tema, primeiro apenas em domínios de ideais principais comutativos, depois estendendo para todos os domínios de integridade comutativos onde uma forma normal de Smith existe sempre (denominados domínios de divisores elementares). Posteriormente, observamos que alguns resultados são válidos no caso não comutativo. No caso do produto, observamos o recurso à localização nos primos, assim como o papel das sequências de Littlewood-Richardson. Notamos a semelhança com outros problemas, nomeadamente, os valores próprios da soma de matrizes hermíticas, e os valores singulares da soma e do produto de matrizes.

Mostramos como certas propriedades de divisibilidade em anéis comutativos também são válidas em anéis em que todos os ideais esquerdos e ideais direitos são bilaterais (anéis duo), tendo como consequência que alguns teoremas relativos a fatores invariantes são aplicáveis nestes anéis.

Palavras-chave: fatores invariantes, forma normal de Smith, anéis de divisores elementares, domínios de divisores elementares, anéis duo

Abstract

The concept of invariant factor of a matrix was introduced in the 19th century by Smith. According to his theorem, any matrix of integers is equivalent to a diagonal matrix, whose entries form a divisibility chain, called Smith normal form. It was then generalised to commutative Principal Ideal Domains. It was also noted the concept applies to more general classes of rings.

Given the invariant factors of two matrices, attempts were made to determine the possible invariant factors of their sum and product. We introduce the main results of this topic, first referring only to commutative principal ideal domains, then extending to all commutative integral domains where a Smith normal form always exists (denominated elementary divisor domains). Later on, we note that some results are valid in the non-commutative case. In the case of the product, we observe the use of localisation at primes, as well as the role of Littlewood-Richardson sequences. We note the similarity with other problems, namely, the eigenvalues of the sum of Hermitian matrices, and the singular values of the sum and the product of matrices.

We show how certain properties of divisibility in commutative rings are also valid for rings where all left ideals and right ideals are bilateral (duo rings), and consequently, some theorems regarding invariant factors can be extended to such rings.

Keywords: invariant factors, Smith normal form, elementary divisor rings, elementary divisor domains, duo rings

Conteúdo

Lista de Figuras

Lista de Símbolos

$M_{m,n}(R)$	matrizes $m \times n$ sobre R 3
$M_n(R)$	matrizes $n \times n$ sobre R 3
$GL_n(R)$	matrizes $n \times n$ invertíveis sobre R 3
$\text{car}(A)$	caraterística de uma matriz 3, 30
$a \mid b$	divide 4, 24
$\text{diag}(\alpha_1, \ldots, \alpha_k)$	matriz diagonal 4
$\text{mdc}(X)$	máximo divisor comum 4, 26
$\text{mmc}(X)$	mínimo múltiplo comum 4, 26
$\det(B)$	determinante de uma matriz 4
R_p	localização de R em p 5
J_k	9
$\lambda(I)$	12
$LR(a, b)$	12
$[a, b]$	intervalo em R 13
$\text{Ann}_R(x)$	anulador 16
$v(x)$	18
$a \sim b$	associados 18, 25
$u(A)$	19, 32
$M_{m,n}(R)_k$	19
$u_\delta(A)$	21
$r_\delta(A)$	21
$a \equiv b \pmod{m}$	22
$\text{Rad}(R)$	radical de Jacobson 25

Introdução

No séc. XIX, ao investigar equações diofantinas, Smith chegou à conclusão que qualquer matriz de números inteiros é equivalente a uma matriz diagonal cujas entradas principais formam uma cadeia de divisibilidade, chamada forma normal de Smith [26, 18]. Às entradas não nulas na diagonal chamamos fatores invariantes da matriz. O teorema de Smith foi aplicado a anéis de polinómios sobre corpos, sendo depois generalizado para quaisquer domínios de ideais principais comutativos. Posteriormente considerou-se estender para classes de anéis mais gerais, nomeadamente os anéis comutativos onde uma forma normal de Smith existe sempre, denominados anéis de divisores elementares, assim como anéis não comutativos, sendo estes investigados por Jacobson [10] e Kaplansky [12].

Foi natural então tentar determinar os possíveis fatores invariantes da soma e do produto de duas matrizes. No que respeita à multiplicação, o problema está completamente resolvido no caso de domínios de ideais principais comutativos. Foi primeiro resolvido por Green e Klein [13], em 1968, um problema equivalente relativo a fatores invariantes de módulos finitamente gerados, tendo descrito a solução usando sequências de Littlewood-Richardson. A equivalência entre esses dois problemas foi mostrada por Thompson [28]. Posteriormente, Azenhas e Sá demonstraram o resultado de Klein com recurso à teoria de matrizes [2]. O problema da adição recebeu atenção nos anos 80, em particular por Thompson [29]. Thompson [28] considerou determinar as relações de divisibilidade entre os fatores invariantes de A, B e AB. Foi nesta formulação alternativa que Carlson e Sá [5] notaram um paralelismo entre este problema e o problema de determinar os valores próprios da soma de duas matrizes hermíticas, assim como o problema de determinar os valores singulares da soma e do produto de duas matrizes complexas. Estes problemas foram todos resolvidos no fim do século. Posteriormente, a generalização destes resultados sobre o problema do produto para domínios de divisores elementares foi contributo de Caldeira e Queiró [3], assim como uma conjetura [4] para a solução do problema da soma, que permanece em aberto.

Esta dissertação está organizada em dois capítulos e tem como tema central os fatores invariantes do produto e da soma de matrizes.

No primeiro capítulo, abordamos os resultados principais conhecidos sobre o tema. Após introdução da noção de fator invariante, focamos no caso do produto. Inicialmente iremos analisar o método de localização nos primos, mostrando que o problema se reduz ao caso local. Seguidamente, introduzimos as sequências de Littlewood-Richardson. Introduzimos então o

problema dos valores próprios da soma de matrizes hermíticas e mostramos a semelhança da sua solução com uma solução do problema dos fatores invariantes do produto, assim como as dos problemas dos valores singulares. São apresentados alguns resultados focando em fatores invariantes individuais, dando ênfase ao paralelismo referido. Introduzimos o conceito de fator invariante de um módulo finitamente gerado sobre um DIP comutativo e mostramos como os problemas de fatores invariantes de matrizes e de módulos são equivalentes.

Seguidamente, introduzimos os domínios de divisores elementares, e discutimos que teoremas anteriores são válidos neste contexto.

Na última secção, apresentamos o caso da soma. Naturalmente refletimos sobre as questões ainda em aberto, em relação às condições necessárias e suficientes.

Iniciamos o segundo capítulo introduzindo os fatores invariantes no caso não comutativo e com existência de divisores de zero, em geral.

Na segunda e última secção do capítulo, é apresentado o nosso contributo para o tema. Refletimos sobre teoremas de Kaplansky, Queiró e Silva entretanto apresentados, analisamos as suas demonstrações e mostramos como se aplicam em anéis mais gerais, nomeadamente anéis de divisores elementares duo, sendo um anel duo quando todos os seus ideais esquerdos e ideais direitos são bilaterais. Com esse objetivo, consideramos proposições gerais em relação à divisibilidade conhecidos no caso comutativo e mostramos a sua validade no caso duo.

Consideramos uma condição suficiente para anéis de Hermite, uma condição suficiente e necessária para ADEs demonstradas por Kaplansky para anéis comutativos, veremos como são válidas ainda em anéis duo.

Revisitamos um teorema de Queiró já apresentado, constituindo numa caracterização específica dos fatores invariantes, tendo sido usada para generalizar proposições para DDEs comutativos. Mostramos como generalizá-lo para o caso duo e com existência de divisores de zero.

Adicionalmente, consideramos quais os anéis duo em que todas as matrizes diagonais têm a redução diagonal canónica, resultando numa observação que demonstra um teorema de Silva em DDEs comutativos.

Fazemos algumas observações sobre os possíveis valores de cada fator invariante individual da soma de matrizes em DDEs comutativos.

Capítulo 1

Fatores invariantes de produtos e somas de matrizes

Importa iniciar a dissertação introduzindo a noção de fatores invariantes.

Seja R um anel (com identidade). Denotamos o conjunto das matrizes $m \times n$ sobre R por $M_{m,n}(R)$, o conjunto das matrizes $n \times n$ sobre R por $M_n(R)$, o conjunto das matrizes $n \times n$ invertíveis sobre R por $GL_n(R)$.

Duas matrizes $A, B \in M_{m,n}(R)$ dizem-se *equivalentes* se $B = PAQ$ para certas $P \in GL_m(R), Q \in GL_n(R)$.

Trocar duas linhas de uma matriz, ou adicionar um múltiplo de uma linha a outra linha, resulta numa matriz equivalente, pois corresponde a multiplicar à esquerda por uma matriz elementar invertível. Multiplicar uma linha por uma unidade u resulta numa matriz equivalente. O mesmo se aplica a colunas.

Seja $A \in M_{m,n}(R)$. A *característica de linha* de A é o número máximo de linhas linearmente independentes de A no R-módulo esquerdo das linhas com n coordenadas. Se A não tiver linhas linearmente independentes, a característica de linha de A é zero. Analogamente, a *característica de coluna* de A é o número máximo de colunas linearmente independentes de A no R-módulo direito das colunas com m coordenadas. Se A não tiver colunas linearmente independentes, A característica de coluna de A é zero.

Se $A \neq 0$, a *característica interna* de A é o menor inteiro positivo k tal que existem matrizes $S \in M_{m,k}(R)$ e $T \in M_{k,n}(R)$ tais que $A = ST$. Se $A = 0$, a característica interna de A é zero.

Se R for comutativo e $A \neq 0$, a *característica determinantal* de A é o maior inteiro positivo k tal que A tem uma submatriz $k \times k$ com determinante não nulo. Se $A = 0$, a característica determinantal de A é zero.

Se o anel R for domínio de integridade comutativo, então as quatro características anteriormente definidas são iguais quer consideremos A como matriz sobre R ou sobre o seu corpo das frações. Denotamo-las por $\mathrm{car}(A)$.

Para matrizes sobre outros anéis, as quatro características podem ser diferentes. Eis alguns exemplos:

Em $\mathbb{Z}_4$:

$$\begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}$$

tem caraterística determinantal 1 e caraterística interna 2.

Em $\mathbb{Z}_{30}$:

$$\begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 3 \end{bmatrix}$$

tem caraterística de linha 2 e caraterística de coluna 1.

Para um anel comutativo R e $a, b \in R$, $a \mid b$ significa a divide b.

Agora seja R um domínio de ideais principais comutativo (DIP). Pode ser mostrado que qualquer matriz $A \in M_{m,n}(R)$ é equivalente a uma matriz diagonal

$$D = \begin{bmatrix} \operatorname{diag}(\alpha_1, \ldots, \alpha_k) & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} \alpha_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \alpha_k & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

onde $\alpha_i \neq 0$, $\alpha_i \mid \alpha_{i+1}$ para $1 \leq i \leq k-1$. Os α_i denominam-se então *fatores invariantes de* A. Diz-se que D é uma *forma normal de Smith de* A, ou simplesmente *redução diagonal de* A.

Dado o i-ésimo fator invariante α_i, um elemento é também i-ésimo fator invariante se e só se for associado a α_i (for obtido de α_i por multiplicação por unidades).

Temos então que duas matrizes são equivalentes se e só se tiverem uma forma normal de Smith em comum.

Por conveniência de notação, se uma matriz A tiver k fatores invariantes (equivalentemente, $\operatorname{car}(A) = k$), denotados por $\alpha_1, \ldots, \alpha_k$, consideramos, para qualquer $i > k$, $\alpha_i = 0$. Dizemos que $(\alpha_i)_{i \in \mathbb{N}}$ é uma *cadeia de fatores invariantes de* A.

No caso de matrizes sobre corpos, como todo o elemento não nulo é unidade, podemos sempre tomar os fatores invariantes como sendo 1s. Logo, no caso $n \times n$, existem exatamente $n+1$ classes de equivalência de matrizes.

Escolhemos um representante de cada classe de associados de R. Em particular, escolhemos 1 como representante da classe das unidades. Se X for um subconjunto de R, os símbolos $\operatorname{mdc}(X)$ e $\operatorname{mmc}(X)$ indicam, respetivamente, os representantes da classes dos máximos divisores comuns e dos mínimos múltiplos comuns de X. Por exemplo, no caso de $\mathbb{Z}$, podemos escolher os inteiros não negativos.

Os fatores invariantes podem ser determinados da seguinte forma: definimos

$$d_i(A) := \operatorname{mdc}\{\det(B) : B \text{ submatriz } i \times i \text{ de } A\} \tag{1.1}$$

Temos que $d_i(A) \mid d_{i+1}(A)$ devido ao teorema de Laplace. Então tomamos $\alpha_i = c$ tal que $d_i(A) = c \cdot d_{i-1}(A)$, com $d_0(A) = 1$ (caso $d_i(A) = d_{i+1}(A) = 0$, tomamos $\alpha_i = 0$).

Exemplo. Consideremos estas duas matrizes em $\mathbb{Z}$:

$$\begin{bmatrix} 2 & 3 \\ 2 & 4 \end{bmatrix}, \begin{bmatrix} 1 & -3 \\ 2 & -4 \end{bmatrix}$$

Ambas têm determinante 2 e têm como entradas números primos entre si, pelo que, por (1.1), os fatores invariantes de ambas são 1 e 2, isto é, multiplicando cada matriz por certas matrizes em $GL_2(\mathbb{Z})$, obtemos:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

Thompson e Sá (independentemente) chegaram ao seguinte resultado sobre os fatores invariantes de submatrizes:

Teorema 1.1 (Desigualdades de Entrelaçamento)**.** *[27, 22] Sejam R um DIP, $A \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $B \in M_{p,q}(R)$ com $p \leq m, q \leq n$ e cujos fatores invariantes são $(\beta_i)_{i\in\mathbb{N}}$. Existe A' equivalente a A tal que contém B como submatriz se e só se, para qualquer i:*

$$\alpha_i \mid \beta_i \mid \alpha_{i+m+n-p-q} \tag{1.2}$$

1.1 Fatores invariantes do produto

Seja R um DIP. Nesta secção, consideramos apenas matrizes quadradas não-singulares (isto é, de caraterística máxima). Consideremos então os n fatores invariantes presentes na redução diagonal da matriz.

O problema principal desta secção consiste em, dados $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in R$ com $\alpha_i \mid \alpha_{i+1}$ e $\beta_i \mid \beta_{i+1}$, determinar as sequências $(\gamma_1, \ldots, \gamma_n) \in R^n$ que são fatores invariantes de uma matriz $C = AB$ não-singular em que A e B são não-singulares e têm fatores invariantes $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ respetivamente. Isto é, desejamos determinar os triplos de sequências $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$, $(\gamma_1, \ldots, \gamma_n) \in R^n$ tais que existem $A, B, C \in M_n(R)$ com fatores invariantes $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$, $(\gamma_1, \ldots, \gamma_n)$ respetivamente, com $C = AB$.

Em particular, procuramos relações de divisibilidade entre os α_i, β_i e γ_i.

Os resultados deste problema generalizam-se ao caso geral [23], isto é, ao problema de determinar os possíveis fatores invariantes de $C = AB$, mesmo quando A, B e C forem matrizes retangulares de caraterística arbitrária.

Definição 1.2. Seja R um DIP. Consideremos um elemento irredutível p de R. A *localização de R em p*, R_p, é o subanel do corpo de quocientes de R gerado por R e os inversos de qualquer elemento irredutível exceto os associados a p. Também pode ser caraterizada por:

$$R_p := \{\frac{a}{b} : a, b \in R, p \not| \, b\} \tag{1.3}$$

Segue-se facilmente:

- $\frac{a}{b}$ é uma unidade se e só se $p \nmid a$
- Qualquer elemento não nulo pode ser expresso como up^i, onde u é uma unidade e $i \in \mathbb{N}_0$
- Qualquer ideal não nulo é gerado por p^i para certo $i \in \mathbb{N}_0$

Uma forma normal de Smith de $A \in M_n(R_p)$ é $\text{diag}(p^{a_1}, \ldots, p^{a_r}, 0, \ldots, 0)$ onde $a_i \in \mathbb{N}_0, a_i \leq a_{i+1}$ e $r = \text{car}(A)$ [8].

Teorema 1.3. *[8] Sejam R um DIP, $p \in R$ irredutível, $A \in M_n(R)$ com fatores invariantes sobre R $\alpha_1, \ldots, \alpha_n$, em que $\alpha_i = p^{a_i}\alpha_i'$ com $p \nmid \alpha_i'$. Então p^{a_i} é um i-ésimo fator invariante de A sobre R_p.*

As potências de p em cada fator invariante de A para cada irredutível p dizem-se *divisores elementares de A.*

Exemplo. Seja $R = \mathbb{Z}$. Consideremos uma matriz com os fatores invariantes $2, 10, 30, 120$. Tem como divisores elementares:

- Para $p = 2$: $2, 2, 2, 8$
- Para $p = 3$: $1, 1, 3, 3$
- Para $p = 5$: $1, 5, 5, 5$
- Para $p = 7$: $1, 1, 1, 1$

Observação 1.4. [8] Para cada classe de associados com elementos irredutíveis em R, selecionamos um representante, e denotamos o conjunto dos representantes por $\mathbb{P}$. Então α_i é associado ao produto dos fatores invariantes sobre R_p de A para cada $p \in \mathbb{P}$.

Teorema 1.5. *[17] Sejam R um DIP, $A, B \in M_n(R)$ não-singulares com fatores invariantes $\alpha_1, \ldots, \alpha_n$; $\beta_1, \ldots, \beta_n$ respetivamente. Sejam $\gamma_1, \ldots, \gamma_n$ fatores invariantes de AB. Então, $\alpha_i \mid \gamma_i$ e $\beta_i \mid \gamma_i$.*

Teorema 1.6. *[17] Sejam R um DIP, $A, B \in M_n(R)$ não-singulares com fatores invariantes $\alpha_1, \ldots, \alpha_n$; $\beta_1, \ldots, \beta_n$ respetivamente tais que $\text{mdc}(\det(A), \det(B)) = 1$, ou, equivalentemente, $\text{mdc}(\alpha_i, \beta_j) = 1$ $\forall 1 \leq i, j \leq n$. Sejam $\gamma_1, \ldots, \gamma_n$ fatores invariantes de AB. Então, γ_i e $\alpha_i\beta_i$ são associados.*

Teorema 1.7. *[2, Teorema 2.1] [28, Pág. 407-408] Seja R um DIP. Sejam $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$, $\gamma_1, \ldots, \gamma_n \in R$ com $\alpha_i \mid \alpha_{i+1}, \beta_i \mid \beta_{i+1}, \gamma_i \mid \gamma_{i+1}$; e $\alpha_i = p^{a_i}\alpha_i'$ com $p \nmid \alpha_i'$, $\beta_i = p^{b_i}\beta_i'$ com $p \nmid \beta_i'$,$\gamma_i = p^{c_i}\gamma_i'$ com $p \nmid \gamma_i'$. As seguintes são equivalentes:*

(a) *Existem $A, B, C \in M_n(R)$ com fatores invariantes sobre R $\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n; \gamma_1, \ldots, \gamma_n$ respetivamente, tais que $C = AB$*

(b) *Para cada p irredutível, existem $A_p, B_p, C_p \in M_n(R_p)$ com fatores invariantes sobre R_p $p^{a_1}, \ldots, p^{a_n}; p^{b_1}, \ldots, p^{b_n}; p^{c_1}, \ldots, p^{c_n}$ respetivamente, tais que $C_p = A_p B_p$*

(c) *Para cada p irredutível, existem $A_p, B_p, C_p \in M_n(R)$ com fatores invariantes sobre R $p^{a_1}, \ldots, p^{a_n}; p^{b_1}, \ldots, p^{b_n}; p^{c_1}, \ldots, p^{c_n}$ respetivamente, tais que $C_p = A_p B_p$*

Observação 1.8. De acordo com o teorema anterior, resolvendo o problema dos fatores invariantes em localizações R_p de DIPs, obtemos uma solução no caso geral. As relações de divisibilidade então tornam-se em desigualdades entre os expoentes de um dado irredutível p, tendo somas em vez de produtos.

1.1.1 Sequências de Littlewood-Richardson

Introduzimos agora alguns conceitos da combinatória, necessários para a descrição de uma solução do problema. Veja, por exemplo, [1].

Definição 1.9. Uma *partição* consiste numa sequência finita de inteiros positivos em ordem decrescente. Por conveniência, podemos adicionar zeros a seguir à sequência (por ex., $(2,1)$ e $(2,1,0,0)$ são consideradas a mesma partição).

Dada uma partição $a = (a_1, \ldots, a_n)$, $|a| := a_1 + \ldots + a_n$, e $l(a)$ denota o número de elementos não nulos na partição. Diz-se que a é uma partição de $|a|$ em $l(a)$ partes.

Usamos a notação $a = (a_1^{x_1}, \ldots, a_n^{x_n})$ para representar a partição em que cada a_i aparece x_i vezes. Por exemplo, $(3^2, 2^3, 1) = (3,3,2,2,2,1)$.

Dada $A \in M_n(R_p)$ não singular com fatores invariantes $p^{a_1}, \ldots, p^{a_n}$; $(a_n, \ldots, a_1)$ é uma partição que se chama *partição invariante de A*.

Uma partição $a = (a_1, \ldots, a_n)$ pode ser representada pelo seu *diagrama de Young*, que é o subconjunto de $\mathbb{N}^2$ definido por

$$\{(i,j) \in \mathbb{N}^2 : 1 \leq i \leq l(a), 1 \leq j \leq a_i\} \tag{1.4}$$

Usualmente é representado por caixas, com i aumentando de cima para baixo, j aumentando da esquerda para a direita.

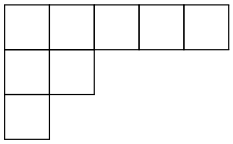

Figura 1.1: Diagrama de Young de $(5,2,1)$

Definição 1.10. Dada uma partição $a = (a_1, \ldots, a_n)$, diz-se que $a^* := (a_1^*, \ldots, a_n^*)$, onde $a_j^* = \#\{i : a_i \geq j\}$, é o *conjugado de a*. Isto é, contam-se as caixas em cada coluna do diagrama de a.

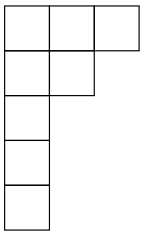

Figura 1.2: Diagrama de Young de $(5,2,1)^* = (3,2,1^3)$

Evidentemente, o diagrama de a^* é o transposto do diagrama de a.

Definição 1.11. [28, Pág. 409-410] [13] Uma sequência de partições (a,b,c) com $l(c) = n$ é uma *sequência de Littlewood-Richardson (LR)* se existirem partições $\sigma^0, \ldots, \sigma^t$ com $l(\sigma^i) \leq n$ (denotamos $\sigma^i = (\sigma^i_1, \ldots, \sigma^i_n)$) tais que:

(a) $\sigma^0 = a$, $\sigma^t = c$

(b) $0 \leq \sigma^{i+1}_j - \sigma^i_j \leq 1$ para todos $0 \leq i \leq t-1$, $1 \leq j \leq n$

(c) $\sum_{j=k}^n (\sigma^{i+1}_j - \sigma^i_j) \geq \sum_{j=k}^n (\sigma^{i+2}_j - \sigma^{i+1}_j)$ para todos $1 \leq k \leq n$, $0 \leq i \leq t-2$

(d) Tomando $m_i := |\sigma^i| - |\sigma^{i-1}|$, temos $b^* = (m_1, \ldots, m_t)$

Exemplo. Consideremos as partições:

$$\sigma^0 := (3,1)$$
$$\sigma^1 := (4,1,1)$$
$$\sigma^2 := (4,2,1,1)$$
$$\sigma^3 := (4,2,2,1)$$

Verificamos que estas partições satisfazem (b) e (c) e que temos $m_1 = 2$, $m_2 = 2$, $m_3 = 1$. Logo, tomando $a = \sigma^0 = (3,1)$, $c = \sigma^3 = (4,2,2,1)$ e $b = (2,2,1)^* = (3,2)$, concluímos que (a,b,c) é uma sequência LR.

Dadas duas partições $a = (a_1, \ldots, a_n)$ e $c = (c_1, \ldots, c_n)$, escrevemos $a \subseteq c$ se $a_i \leq c_i$. Isto quer dizer que o diagrama de a está contido no diagrama de c.

Definição 1.12. [1] Se $a \subseteq c$, define-se o *diagrama enviesado de Young*:

$$c/a := \{(i,j) \in c : (i,j) \notin a\} \tag{1.5}$$

Definição 1.13. [1] Um *tableau de Young* consiste no diagrama enviesado de Young c/a em que a cada caixa (i,j) se associa um número $\tau_{i,j} \in \{1, \ldots, t\}$ ($t \in \mathbb{N}$), com as propriedades $\tau_{i,j} < \tau_{i,j+1}$, $\tau_{i,j} \leq \tau_{i+1,j}$ (ordem crescente de cima para baixo e estritamente crescente da esquerda para a direita).

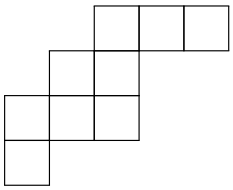

Figura 1.3: Diagrama enviesado de Young c/a com $c = (5, 3, 3, 1), a = (2, 1, 0, 0)$

Dado um tableau de Young T, seja $m_k := \#\{(i, j) : \tau_{i,j} = k\}, 1 \leq k \leq t$. Podemos ordenar os m_k por ordem decrescente, isto é, existe uma partição $b = (b_1, \ldots, b_t)$ tal que $b_k = m_{\sigma(k)}$ onde $\sigma \in S_t$ (permutação de t símbolos). Dizemos então que T é de *tipo* (a, b^*, c), ou que tem *forma* c/a e *peso* b^*. Para pôr o ênfase na permutação, dizemos que é um σ*-tableau*.

		1	2	3
	2	3		
1	2	4		
3				

Figura 1.4: σ-Tableau de Young to tipo (a, b^*, c), com $a = (2, 1, 0, 0)$, $c = (5, 3, 3, 1)$, $b^* = (3, 3, 2, 1)$, $\sigma = (1\ 3)$

Definição 1.14. [1] Definimos para $1 \leq k \leq t$, $J_k := \{i : \exists j : \tau_{i,j} = k\}$ (índices das linhas que contêm uma caixa com k).

Temos, para o exemplo na figura 1.4, $J_1 = \{1, 3\}, J_2 = \{1, 2, 3\}, J_3 = \{1, 2, 4\}, J_4 = \{3\}$

Pela definição de tableau de Young, existe no máximo uma caixa com k em cada linha, logo $m_k = \#J_k$ e $b = (\#J_{\sigma(1)}, \ldots, \#J_{\sigma(t)})$.

Dado um tableau T com forma c/a, consideramos T_i o diagrama de Young de a unido com o conjunto das caixas com números $\leq i$ em T. T_i é um diagrama de Young e representa uma partição a_i. T é completamente definido pelos a_i e podemos escrever $T = (a_0, \ldots, a_t)$ (note-se que $a_0 = a$ e $a_t = c$).

Na figura 1.4, $a_0 = a = (2, 1, 0, 0)$. Temos $a_1 = (3, 1, 1, 0)$, notando que existem 1s nas linhas 1 e 3. Com observações semelhantes, obtemos $a_2 = (4, 2, 2, 0)$, $a_3 = (5, 3, 2, 1)$, $a_4 = c = (5, 3, 3, 1)$.

Consideremos agora a seguinte ordem parcial sobre subconjuntos finitos de $\mathbb{N}$: dados $A = \{a_1, \ldots, a_n\}, B = \{b_1, \ldots, b_m\}$, com $a_i > a_{i+1}$ e $b_i > b_{i+1}$; definimos:

$$A \geq B \text{ se } n \geq m \text{ e } a_i \geq b_i \text{ para } 1 \leq i \leq m \tag{1.6}$$

Note-se que $A \geq B$ se e só se existir $C \subseteq A$ tal que $\#C = \#B$ e $C \geq B$.

Definição 1.15. [1] Um tableau de Young diz-se um *tableau de Littlewood-Richardson (tableau LR)* se:

$$J_1 \geq J_2 \geq \ldots \geq J_t \tag{1.7}$$

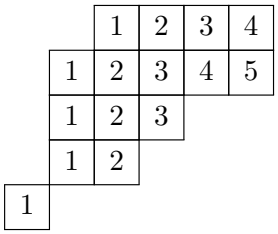

Figura 1.5: Exemplo de tableau LR. Temos $J_1 = \{1,2,3,4,5\}, J_2 = \{1,2,3,4\}, J_3 = \{1,2,3\}, J_4 = \{1,2\}, J_5 = \{2\}$. Facilmente se vê que $J_1 \geq J_2 \geq \ldots \geq J_5$.

Teorema 1.16. *[1, Pág. 67] (a,b,c) é uma sequência LR se e só se existir um tableau LR de tipo (a,b,c).*

As sequências LR mostraram-se relevantes na obtenção de resultados do problema dos fatores invariantes do produto de matrizes. Apresentamos então um dos resultados principais da secção:

Teorema 1.17. *[13] [28, Pág. 410] Sejam R um DIP, $p \in R$ irredutível. Existem $A, B, C \in M_n(R_p)$ não-singulares com partições invariantes a, b e c respetivamente tais que $AB = C$ se e só se (a,b,c) for uma sequência LR.*

Mais especificamente, prova-se que:

Teorema 1.18. *[13] [2, Pág. 234-235] Sejam R um DIP, $p \in R$ irredutível. Dado um tableau LR $T = (a_0, \ldots, a_t)$ de tipo (a,b,c) com $l(c) \leq n$ e $b^* = (b_1, \ldots, b_t)$ existem $A, B_1, \ldots B_t \in M_n(R_p)$ não-singulares tais que:*

(a) *A tem partição invariante a*

(b) *$A_i := AB_1 \cdots B_i$ tem partição invariante a_i*

(c) *B_i tem partição invariante (1^{b_i})*

(d) *$B := B_1 \cdots B_t$ tem partição invariante b*

Também se prova que qualquer fatorização de B com as propriedades acima corresponde ao mesmo tableau.

A sequência de matrizes $A, B_1, \ldots B_t$ diz-se uma *realização matricial do tableau T*.

Tomando $C = A_t = AB_1 \cdots B_t = AB$ e notando que $a_t = c$, vemos que este teorema especifica a existência das matrizes procuradas quando (a,b,c) for uma sequência LR.

1.1.2 Valores próprios de somas de matrizes hermíticas

Iremos analisar um problema que tem muito em comum com o problema dos fatores invariantes do produto e contribuiu para a sua resolução.

Recorde-se que uma matriz $A \in M_n(\mathbb{C})$ diz-se *hermítica* se $A^H = A$ (A^H denota a conjugada da transposta de A). Matrizes hermíticas têm valores próprios reais e são semelhantes a matrizes diagonais reais. Ordenamos os valores próprios por ordem decrescente.

Denotamos $\Lambda_n := \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 \geq \ldots \geq x_n\}$.

Consideremos então o problema de encontrar as sequências $(a_1, \ldots, a_n)$,$(b_1, \ldots, b_n)$,$(c_1, \ldots, c_n) \in \Lambda_n$ tais que são valores próprios de matrizes hermíticas $A, B, C \in M_n(\mathbb{C})$ respetivamente, com $C = A + B$.

Com o objetivo de obter uma descrição da solução do problema, identificaram-se subconjuntos I, J, K de $\{1, \ldots, n\}$ com $\#I = \#J = \#K$ para os quais, para quaisquer $A, B \in M_n(\mathbb{C})$ com valores próprios $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ respetivamente, sendo $c_1, \ldots, c_n$ os valores próprios de $A + B$:

$$\sum_{k \in K} c_k \leq \sum_{i \in I} a_i + \sum_{j \in J} b_j \tag{1.8}$$

Note-se que temos a igualdade no caso $I = J = K = \{1, \ldots, n\}$, pois o traço de uma matriz é igual à soma dos seus valores próprios.

Dada uma desigualdade (1.8) e a igualdade referida, podemos obter outra desigualdade:

$$\sum_{i \in I^C} a_i + \sum_{j \in J^C} b_j \leq \sum_{k \in K^C} c_k \tag{1.9}$$

(onde, para $L \subseteq \{1, \ldots, n\}$, L^C denota $\{1, \ldots, n\} \backslash L$).

Procurava-se obter um conjunto independente de desigualdades, isto é, em que nenhuma das desigualdades é consequência das restantes. É possível obter uma descrição da solução do problema usando apenas desigualdades do tipo (1.8) mais a igualdade do traço referida acima.

A solução deste problema foi conjeturada por Horn nos anos 50.

Definimos:

$$U_r^n := \{(I, J, K) : I, J, K \subseteq \{1, \ldots, n\}, \#I = \#J = \#K = r, \sum_{i \in I} i + \sum_{j \in J} j = \sum_{k \in K} k + \frac{r(r+1)}{2}\} \tag{1.10}$$

Definimos agora T_r^n recursivamente. Pomos $T_1^n := U_1^n$, e:

$$T_r^n := \{(I, J, K) \in U_r^n : \ \forall p < r \ \forall (F, G, H) \in T_p^r \ \sum_{f \in F} i_f + \sum_{g \in G} j_g \leq \sum_{h \in H} k_h + \frac{p(p+1)}{2}\} \tag{1.11}$$

Horn conjeturou que a solução no caso $n \times n$ é definida pelas desigualdades (1.8) dadas pelos conjuntos em $\bigcup_{r=1}^{n-1} T_r^n$ assim como a igualdade dos traços [7, Pág. 212]. Note-se no entanto que este conjunto de desigualdades e igualdade não é independente em geral. De facto, só é independente para $n \leq 5$ [7, Pág. 214].

A sua conjetura foi demonstrada em 1998 por Klyachko [14]. Mais, revelou-se possível também exprimir a solução a partir das sequências LR.

Dado um conjunto $I = \{i_1, \ldots, i_r\} \subset \mathbb{N}$, com $i_j < i_{j+1}$ definimos a partição:

$$\lambda(I) := (i_r - r, i_{r-1} - (r-1), \ldots, i_1 - 1) \tag{1.12}$$

Denotamos o conjunto das partições c tal que (a, b, c) é uma sequência LR por $LR(a, b)$.

Teorema 1.19. *[7, Teorema 12] Para qualquer $r < n$, os subconjuntos I, J, K de $\{1, \ldots, n\}$ com $\#I = \#J = \#K = r$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$ são exatamente os subconjuntos tais que $(I, J, K) \in T_r^n$.*

Teorema 1.20. *[7, Pág. 212-213] As desigualdades (1.8) para todos I, J, K subconjuntos de $\{1, \ldots, n\}$ com $\#I = \#J = \#K$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$, mais a igualdade no caso $I = J = K = \{1, \ldots, n\}$, definem exatamente a solução do problema. Isto é, $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$,$(c_1, \ldots, c_n) \in \Lambda_n$ são valores próprios de $A, B, C \in M_n(\mathbb{C})$ hermíticas com $C = A+B$ se e só se tivermos (1.8) para todos I, J, K subconjuntos de $\{1, \ldots, n\}$ com $\#I = \#J = \#K$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$, assim como a igualdade no caso $I = J = K = \{1, \ldots, n\}$.*

Por exemplo, no caso $n = 2$, as seguintes condições definem completamente os possíveis valores próprios da soma de duas matrizes hermíticas:

- $c_1 + c_2 = a_1 + a_2 + b_1 + b_2$
- $c_1 \leq a_1 + b_1$
- $c_2 \leq a_2 + b_1$
- $c_2 \leq a_1 + b_2$

1.1.3 Outra solução do problema

Voltemos ao problema principal desta secção, o problema dos fatores invariantes do produto.

Com o objetivo de apresentarmos uma solução alternativa do problema, focamos novamente na localização R_p. Denominamos agora os a_i, b_i e c_i como sendo os elementos das partições invariantes de A, B e AB respetivamente, isto é, os expoentes (de p) dos fatores invariantes, mas na ordem oposta.

Thompson [28] procurou encontrar desigualdades do tipo (1.8). Acontece que o problema tem a mesma solução que o problema dos valores próprios:

Teorema 1.21. *[7, Teorema 7] [3] Sejam R um DIP, $p \in R$ irredutível. As desigualdades (1.8) para todos I, J, K subconjuntos de $\{1, \ldots, n\}$ com $\#I = \#J = \#K$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$, mais a igualdade no caso $I = J = K = \{1, \ldots, n\}$, definem exatamente a solução do problema. Isto é, $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$,$(c_1, \ldots, c_n)$ são partições invariantes de $A, B, C \in M_n(R_p)$ com $C = AB$ se e só se tivermos (1.8) para todos I, J, K subconjuntos de $\{1, \ldots, n\}$ com $\#I = \#J = \#K$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$, assim como a igualdade no caso $I = J = K = \{1, \ldots, n\}$.*

Observação 1.22. Posto de outra forma, dadas $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ partições denotamos $IF(a, b)$ o subconjunto de $\mathbb{N}_0^n$ cujos elementos correspondem a partições invariantes de $C \in M_n(R_p)$ tais que $A, B \in M_n(R_p)$ têm partições invariantes a e b respetivamente, e $C = AB$. Denotamos $E(a, b)$ o subconjunto de Λ_n cujos elementos correspondem a valores próprios de $C \in M_n(\mathbb{C})$ hermítica tais que $A, B \in M_n(\mathbb{C})$ hermíticas têm valores próprios $(a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n)$ respetivamente, e $C = A + B$. Então, temos:

$$IF(a, b) = E(a, b) \cap \mathbb{N}_0^n \tag{1.13}$$

1.1.4 Fatores invariantes individuais

Agora focamos num único fator invariante de AB.

Teorema 1.23. *[20] Seja R um DIP, sejam $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n, \gamma \in R$ com $\alpha_i \mid \alpha_{i+1}, \beta_i \mid \beta_{i+1}$. Existem $A, B \in M_n(R)$ não-singulares com fatores invariantes $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ tais que γ é um k-ésimo fator invariante de AB se e só se:*

$$\operatorname{mmc}(\alpha_{k-i}\beta_{i+1} : 0 \leq i \leq k-1) \mid \gamma \mid \operatorname{mdc}(\alpha_{n-i+1}\beta_{k+i-1} : 1 \leq i \leq n-k+1) \tag{1.14}$$

Então, podemos exprimir o conjunto de elementos possíveis de ser fatores invariantes de AB como uma união de intervalos em R, como se define a seguir.

Para $a, b \in R$ definimos $[a, b] := \{x \in R : a \mid x \mid b\}$

Temos:

Corolário 1.24. *[20] Seja R um DIP, sejam $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n, \gamma \in R$ com $\alpha_i \mid \alpha_{i+1}, \beta_i \mid \beta_{i+1}$. Existem $A, B \in M_n(R)$ não-singulares com fatores invariantes $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ tais que γ é um fator invariante de AB se e só se:*

$$\gamma \in \bigcup_{k=1}^{n} [\operatorname{mmc}(\alpha_{k-i}\beta_{i+1} : 0 \leq i \leq k-1), \operatorname{mdc}(\alpha_{n-i+1}\beta_{k+i-1} : 1 \leq i \leq n-k+1)] \tag{1.15}$$

Considerando agora uma localização R_p, denominamos a_i e b_i como sendo os expoentes (de p) dos fatores invariantes de A e B respetivamente, por ordem crescente. As condições 1.14 e 1.15 implicam as seguintes que envolvem estes expoentes e também o expoente c de p em γ.

$$\max(a_{k-i} + b_{i+1} : 0 \leq i \leq k-1) \leq c \leq \min(a_{n-i+1} + b_{k+i-1} : 1 \leq i \leq n-k+1) \tag{1.16}$$

$$c \in \bigcup_{k=1}^{n} [\max(a_{k-i} + b_{i+1} : 0 \leq i \leq k-1), \min(a_{n-i+1} + b_{k+i-1} : 1 \leq i \leq n-k+1)] \tag{1.17}$$

Esta última expressão pode ser simplificada:

Teorema 1.25. *[20] Sejam R um DIP, $p \in R$ irredutível. Sejam $a_1, \ldots, a_n, b_1, \ldots, b_n, c \in \mathbb{N}$ com $a_i \leq a_{i+1}, b_i \leq b_{i+1}$. Existem $A, B \in M_n(R_p)$ não-singulares com fatores invariantes $p^{a_1}, \ldots, p^{a_n}$ e $p^{b_1}, \ldots, p^{b_n}$ tais que p^c é um fator invariante de AB se e só se:*

$$c \in (\bigcup_{k=1}^{n} [a_k + b_1, a_k + b_n]) \cap (\bigcup_{r=1}^{n} [a_1 + b_r, a_n + b_r]) \tag{1.18}$$

Observação 1.26. [11] [7, Pág. 215] Podemos fazer uma observação semelhante em relação aos valores próprios da soma de matrizes hermíticas, ordenados por ordem decrescente. Dadas $A, B \in M_n(\mathbb{C})$ hermíticas, os possíveis valores para o k-ésimo valor próprio c de $A+B$ são dados por:

$$\max(a_{k+i} + b_{n-i} : 0 \leq i \leq n-k) \leq c \leq \min(a_i + b_{k-i+1} : 1 \leq i \leq k) \tag{1.19}$$

1.1.5 Valores singulares

Recorde-se que, dada $A \in M_{m,n}(\mathbb{C})$, $A = UDV$, onde $U \in M_m(\mathbb{C})$, $V \in M_n(\mathbb{C})$ são matrizes unitárias, $D \in M_{m,n}(\mathbb{C})$ é diagonal com elementos diagonais $\sigma_1, \ldots, \sigma_q$ $(q = \min(m,n))$, os quais denominamos os *valores singulares de* A. Ordenamos os valores singulares por ordem decrescente.

Teorema 1.27. *[7, Teorema 16] Sejam $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, $c_1, \ldots, c_n \in \mathbb{R}$ não negativos com $a_i \geq a_{i+1}, b_i \geq b_{i+1}, c_i \geq c_{i+1}$. Existem $A, B \in M_n(\mathbb{C})$ com valores singulares $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ respetivamente tais que $c_1, \ldots, c_n$ são valores singulares de AB se e só se*

$$\prod_{k \in K} c_k \leq \prod_{i \in I} a_i \prod_{j \in J} b_j \tag{1.20}$$

para todos I, J, K subconjuntos de $\{1, \ldots, n\}$ com $\#I = \#J = \#K$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$.

Podemos deduzir, como para fatores invariantes, resultados pertinentes a cada valor singular individual:

Teorema 1.28. *[20] Sejam $a_1, \ldots, a_n, b_1, \ldots, b_n, c \in \mathbb{R}$ não negativos com $a_i \geq a_{i+1}, b_i \geq b_{i+1}$. Existem $A, B \in M_n(\mathbb{C})$ com valores singulares $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ respetivamente tais que c é o k-ésimo valor singular de AB se e só se:*

$$\max\{a_{k-i} b_{n-i} : 0 \leq i \leq n-k\} \leq c \leq \min\{a_i b_{k-i+1} : 1 \leq i \leq k\} \tag{1.21}$$

Os possíveis valores singulares de AB são, então:

$$c \in \bigcup_{k=1}^{n} [\max\{a_{k-i} b_{n-i} : 0 \leq i \leq n-k\}, \min\{a_i b_{k-i+1} : 1 \leq i \leq k\}] \tag{1.22}$$

Tal como no caso dos fatores invariantes, pode ser expresso alternativamente: [20]

$$c \in (\bigcup_{k=1}^{n} [a_k b_n, a_k b_1]) \cap (\bigcup_{r=1}^{n} [a_n b_r, a_1 b_r]) \tag{1.23}$$

1.1.6 Valores singulares da soma de matrizes

Dada $A \in M_{m,n}(\mathbb{C})$ com valores singulares $\sigma_1, \ldots, \sigma_q$ $(q := \min(m,n))$, temos que os valores próprios da matriz $(m+n) \times (m+n)$ hermítica

$$\begin{bmatrix} 0 & A \\ A^H & 0 \end{bmatrix} \tag{1.24}$$

são $\sigma_1, \ldots, \sigma_q, 0, \ldots, 0, -\sigma_q, \ldots, -\sigma_1$, com $|m-n|$ zeros [7, Pág. 225].

Esta proposição permite-nos deduzir desigualdades para os valores singulares de $A+B$ a partir das desigualdades para os valores próprios. Observe-se que, tal como para os valores próprios, estas desigualdades determinam completamente os possíveis valores singulares.

Para $I, J, K \subseteq \{1, \ldots, m+n\}$, seja $I' := \{i \in \{1, \ldots, m+n\} : m+n+1-i \in I\}$ (os índices dos valores singulares de A correspondendo a valores próprios negativos). Definimos J' e K' analogamente. Sejam $a_1, \ldots, a_q$; $b_1, \ldots, b_q$; $c_1, \ldots, c_q$ os valores singulares de A, B e $A+B$ respetivamente. Se tivermos (1.8) para certos I, J, K, então obtemos:

$$\sum_{\substack{i \in I \\ i \leq q}} a_i - \sum_{\substack{i \in I' \\ i \leq q}} a_i + \sum_{\substack{j \in J \\ j \leq q}} b_j - \sum_{\substack{j \in J' \\ j \leq q}} b_j \geq \sum_{\substack{k \in K \\ k \leq q}} c_k - \sum_{\substack{k \in K' \\ k \leq q}} c_k \tag{1.25}$$

Teorema 1.29. *[7, Teorema 15] Sejam $a_1, \ldots, a_q$, $b_1, \ldots, b_q$, $c_1, \ldots, c_q \in \mathbb{R}$ não negativos com $a_i \geq a_{i+1}, b_i \geq b_{i+1}, c_i \geq c_{i+1}$. Existem $A, B \in M_{m,n}(\mathbb{C})$ com valores singulares $a_1, \ldots, a_q$ e $b_1, \ldots, b_q$ respetivamente tais que $c_1, \ldots, c_q$ são valores singulares de $A+B$ se e só se (1.25) para todos I, J, K subconjuntos de $\{1, \ldots, m+n\}$ com $\#I = \#J = \#K$ tais que $\lambda(K) \in LR(\lambda(I), \lambda(J))$.*

Analisando cada valor singular individual:

Teorema 1.30. *[20] Sejam $a_1, \ldots, a_n, b_1, \ldots, b_n, c \in \mathbb{R}$ não negativos com $a_i \geq a_{i+1}, b_i \geq b_{i+1}$. Existem $A, B \in M_n(\mathbb{C})$ com valores singulares $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ respetivamente tais que c é o k-ésimo valor singular de $A+B$ se e só se:*

$$\max\{a_{k+i} - b_{i+1}, b_{k+i} - a_{i+1}, 0 : 0 \leq i \leq n-k\} \leq c \leq \min\{a_i + b_{k-i+1} : 1 \leq i \leq k\} \tag{1.26}$$

Temos então que os valores singulares de $A+B$ possíveis são dados por:

$$c \in \mathbb{R}_0^+ \cap \left(\bigcup_{k=1}^{n} [\max\{a_{k+i} - b_{i+1}, b_{k+i} - a_{i+1} : 0 \leq i \leq n-k\}, \min\{a_i + b_{k-i+1} : 1 \leq i \leq k\}]\right) \tag{1.27}$$

Tal como no caso do produto, pode ser expresso alternativamente:

$$c \in \mathbb{R}_0^+ \cap \left(\bigcup_{k=1}^{n} [a_k - b_1, a_k + b_1]\right) \cap \left(\bigcup_{r=1}^{n} [b_r - a_1, b_r + a_1]\right) \tag{1.28}$$

Podemos assumir sem perda de generalidade que $a_1 \geq b_1$, segue-se que o último termo da interseção contém $[0, a_1 + b_1]$ o que por sua vez contém a interseção dos outros dois. Portanto:

$$c \in \mathbb{R}_0^+ \cap \left(\bigcup_{k=1}^{n} [a_k - b_1, a_k + b_1]\right) \tag{1.29}$$

1.1.7 Módulos

Introduzimos o conceito de fatores invariantes de um módulo finitamente gerado sobre um DIP, de modo a mostrar a equivalência entre os problemas dos fatores invariantes nas matrizes e nos módulos.

Definição 1.31. Sejam R um DIP, M um R-módulo, $x \in M$. Definimos o *anulador de* x como $\mathrm{Ann}_R(x) := \{a \in R : ax = 0\}$.

Facilmente se mostra que $\mathrm{Ann}_R(x)$ é um ideal de R.

Definição 1.32. Chamamos *ordem de* x, $o(x)$, a qualquer gerador de $\mathrm{Ann}_R(x)$.

Definição 1.33. Diz-se que x é um *elemento de torção* se $\mathrm{Ann}_R(x) \neq \{0\}$ ou, equivalentemente, $o(x) \neq 0$. Define-se M_t o conjunto dos elementos de torção de M.

Facilmente se mostra que M_t é um submódulo de M.

Teorema 1.34. *Sejam R um DIP, M um R-módulo finitamente gerado. Existem $x_1, \ldots, x_n \in M_t \backslash \{0\}$ tais que:*

$$M = L \oplus Rx_1 \oplus \ldots \oplus Rx_n \tag{1.30}$$

onde $o(x_i) \mid o(x_{i+1})$, com L submódulo livre de M.

Se temos $y_1, \ldots, y_m \in M_t \backslash \{0\}$ tais que:

$$M = L' \oplus Ry_1 \oplus \ldots \oplus Ry_m \tag{1.31}$$

onde $o(y_i) \mid o(y_{i+1})$, com L' submódulo livre de M; então $n = m$, $L \cong L'$ e $Rx_i \cong Ry_i$. Isto é, a decomposição é única a menos de isomorfismo das componentes.

Esta decomposição chama-se então a *decomposição de M em fatores invariantes*, e os $o(x_i)$ denominam-se os *fatores invariantes de M*.

Definição 1.35. [28, Pág. 403] Sejam R um DIP, M um R-módulo finitamente gerado. Sejam $x_1, \ldots, x_n$ geradores de M. Denotamos $x := \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^T$. Então $r := \begin{bmatrix} r_1 & \cdots & r_n \end{bmatrix} \in M_{1,n}(R)$ diz-se uma *relação* se $rx = \sum_{i=1}^{n} r_i x_i = 0$

Definição 1.36. [28, Pág. 403] $A \in M_{m,n}(R), A = [a_{i,j}]$ diz-se uma *matriz de relações* se $Ax = 0$, isto é $\sum_{j=1}^{n} a_{i,j} x_j = 0 \ \forall i$ (as suas linhas forem relações). Se, para qualquer relação r, $r = yA$ para $y \in M_{1,m}(R)$ (isto é, qualquer relação for combinação linear das linhas de A), A diz-se uma *matriz de relações completa*.

Dado um módulo finitamente gerado, existe sempre uma matriz de relações completa. Também temos o recíproco, isto é, dada uma matriz A, existe um módulo finitamente gerado para o qual A é uma matriz de relações completa [28, Pág. 403].

Podemos desenvolver o conceito:

Teorema 1.37. *[28, Pág. 406] Seja R um DIP. Dadas matrizes A, B, C sobre R com $C = AB$, existe um R-módulo finitamente gerado M e N submódulo de M tais que A, B e C são matrizes de relação completa de N, M/N e M respetivamente.*

Teorema 1.38. *[28, Pág. 406] Sejam R um DIP, M um R-módulo finitamente gerado, N um submódulo de M. Existem matrizes (sobre R) A, B e C sendo matrizes de relação completa de N, M/N e M respetivamente, tais que $C = AB$.*

Teorema 1.39. *[28, Pág. 405] Seja R um DIP. Os fatores invariantes de um R-módulo finitamente gerado são os fatores invariantes excluindo unidades de qualquer sua matriz de relações completa.*

Observação 1.40. [28, Pág. 405] Se tomarmos os geradores $x_1, \ldots, x_n$ que formam a decomposição (1.30), então existe uma matriz de relações completa diagonal na forma normal de Smith, cujos elementos diagonais não nulos são $o(x_i)$, ou seja, os fatores invariantes de M. Os zeros no fim da diagonal correspondem a elementos que formam uma base de L.

Combinando os resultados anteriores, obtemos:

Teorema 1.41. *[28, Pág. 407] Seja R um DIP. Sejam $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n, \gamma_1, \ldots, \gamma_n \in R$. Existem $A, B, C \in M_n(R)$ não-singulares com fatores invariantes $\alpha_1, \ldots, \alpha_n$; $\beta_1, \ldots, \beta_n$ e $\gamma_1, \ldots, \gamma_n$ respetivamente, tais que $C = AB$ se e só se existir um R-módulo finitamente gerado N com fatores invariantes $\gamma_1, \ldots, \gamma_n$, no qual existe um submódulo P com fatores invariantes $\alpha_1, \ldots, \alpha_n$ tal que N/P tem fatores invariantes $\beta_1, \ldots, \beta_n$.*

Definição 1.42. Um R-módulo M diz-se um *p-módulo* para $p \in R$ irredutível se $p^e M = \{0\}$ para algum $e \in \mathbb{N}$. O menor e tal que $p^e M = \{0\}$ chama-se o *expoente de M*.

Teorema 1.43. *[28, Pág. 407] Seja R um DIP, M um R-módulo. Então:*

$$M = \bigoplus_p M_p \tag{1.32}$$

em que cada M_p é um p-módulo.

Se N for um submódulo de M, temos

$$N = \bigoplus_p N_p \tag{1.33}$$

em que cada N_p é um p-módulo e um submódulo de M_p. Também temos:

$$M/N = \bigoplus_p M_p/N_p \tag{1.34}$$

Isto corresponde à fatorização por irredutíveis das matrizes e seus fatores invariantes vista no teorema 1.7. Green e Klein [13] resolveram o problema de fatores invariantes de módulos lidando com p-módulos.

1.2 Domínios de divisores elementares

Consideremos agora uma classe de anéis maior:

Definição 1.44 (Domínio de divisores elementares)**.** [12] Um anel comutativo R diz-se um *domínio de divisores elementares (DDE)* se for um domínio de integridade e se toda a matriz A sobre R tiver forma normal de Smith, isto é, for equivalente a uma matriz diagonal

$$D = \begin{bmatrix} \operatorname{diag}(\alpha_1, \ldots, \alpha_k) & 0 \\ 0 & 0 \end{bmatrix}$$

onde $\alpha_i \neq 0$, $\alpha_i \mid \alpha_{i+1}$ para $1 \leq i \leq k-1$.

Observação 1.45. Como no caso dos DIPs, os fatores invariantes α_i são únicos a menos de associados, e podem ser obtidos pelos divisores determinantais $d_i(A)$ da mesma maneira.

Um exemplo de um DDE que não é um DIP é $H(\Omega)$, o anel de funções complexas holomorfas num conjunto $\Omega \subseteq \mathbb{C}$ aberto e conexo [3].

Definição 1.46. Um anel R diz-se um *anel de MDC* se para todo $a, b \in R$, existir mdc de $\{a, b\}$.

Definição 1.47. Um anel comutativo R diz-se um *anel de Bézout* se todo o ideal finitamente gerado for principal.

Um anel de Bézout comutativo é um anel de MDC, sendo o mdc sempre uma combinação linear de a e b. Em geral, um mdc de $\{a, b\}$ não é necessariamente uma combinação linear de a e b.

O seguinte é uma proposição relativa a anéis de Bézout, relevante para o tema:

Teorema 1.48. *[16, Teorema 3.1] Seja R um anel comutativo. Todas as matrizes quadradas diagonais sobre R têm forma normal de Smith se e só se R for um anel de Bézout.*

Apresentamos então a seguinte condição suficiente e necessária para DDEs:

Teorema 1.49. *[12, Teorema 5.2] Seja R um domínio de integridade comutativo. R é um DDE se e só se:*

(a) *For um anel de Bézout.*

(b) *Para $a, b, c \in R$ tais que $\operatorname{mdc}(a, b, c) = 1$, existirem $p, q \in R$ tais que $\operatorname{mdc}(pa, pb + qc) = 1$.*

Queiró pretendeu estender alguns teoremas conhecidos para DDEs. A seguir, expomos um teorema que foi usado com esse objetivo.

Definimos uma "norma" para vetores e matrizes sobre R [19].

Para $x \in R^n, x = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^T$, definimos $v(x) := \operatorname{mdc}(x_1, \ldots, x_n)$.

Nas seguintes proposições, para $a, b \in R$, $a \sim b$ denota igualdade a menos de multiplicação por unidades. Prova-se facilmente em DDEs:

(a) $x \neq 0 \Rightarrow v(x) \neq 0$

(b) $v(ax) \sim av(x)\ \forall a \in R$

(c) $\mathrm{mdc}(v(x), v(y)) \mid v(x+y)$

(d) $v(x) \mid v(Ax)\ \forall A \in M_{m,n}(R)$

(e) $v(x) = v(Ux)\ \forall U \in GL_n(R)$

Agora para $A \in M_{m,n}(R)$, $A = [a_{i,j}]$, definimos $u(A) := \mathrm{mdc}\{a_{i,j} : 1 \leq i \leq m, 1 \leq j \leq n\}$. Provam-se facilmente as seguintes proposições:

(a) $A \neq 0 \Rightarrow u(A) \neq 0$

(b) $u(aA) \sim au(A)\ \forall a \in R$

(c) $\mathrm{mdc}(u(A), u(B)) \mid u(A+B)$

(d) $u(A)u(B) \mid u(AB)$

(e) $u(A) = u(UAV)\ \forall U \in GL_m(R)\ \forall V \in GL_n(R)$

Em [19], Queiró de facto definiu $u(A)$ como no lema seguinte, que mostra a equivalência das definições. Optámos pela primeira definição para clarificar a validade em DDEs das proposições acima.

Lema 1.50. *Seja R um DDE. Para $A \in M_{m,n}(R)$, temos:*

$$u(A) = \mathrm{mdc}\{v(Ax) : x \in R^n\} \tag{1.35}$$

Demonstração. Seja $x \in R^n$, $x = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^T$ e definimos $e_i \in R^n$ o vetor com i-ésima componente 1 e 0 nas restantes. Então $Ax = \sum_{i=1}^{n} x_i Ae_i$. Note-se que Ae_i é a i-ésima coluna de A, portanto: $u(A) = \mathrm{mdc}\{v(Ae_i) : 1 \leq i \leq n\} \mid \mathrm{mdc}\{v(x_i Ae_i) : 1 \leq i \leq n\} \mid v(\sum_{i=1}^{n} x_i Ae_i) = v(Ax)$

Seja $a \in R$ tal que $a \mid v(Ax)\ \forall x \in R^n$. Então $a \mid v(Ae_i)\ \forall 1 \leq i \leq n$, logo $a \mid \mathrm{mdc}\{v(Ae_i) : 1 \leq i \leq n\} = u(A)$. □

Denotamos $M_{m,n}(R)_k := \{A \in M_{m,n}(R) : \mathrm{car}(A) < k\}$.

Teorema 1.51. *[19] Seja R um DDE. Seja $A \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i \in \mathbb{N}}$. Então:*

$$\alpha_k \sim \mathrm{mmc}\{u(A - X) : X \in M_{m,n}(R)_k\} \tag{1.36}$$

1.2.1 Fatores invariantes do produto em DDEs

Agora, referindo aos fatores invariantes de um produto de matrizes, tentou-se encontrar desigualdades do tipo:

$$\prod_{k\in K}\gamma_k \mid \prod_{i\in I}\alpha_i \prod_{j\in J}\beta_j \tag{1.37}$$

onde I, J, K são subconjuntos de $\{1,\dots,n\}$ com $\#I = \#J = \#K$.

Note-se que temos a igualdade a menos de multiplicação por unidades, no caso $I = J = K = \{1,\dots,n\}$, tomando os determinantes. Se R for uma localização R_p, então as desigualdades acima reduzem-se a desigualdades do tipo (1.8) (recordamos no entanto que o i-ésimo fator invariante tem como expoente de p o $n-i+1$-ésimo elemento da partição invariante). Se R for um DIP, combinando a mesma desigualdade tipo (1.37) em R_p para todos os elementos irredutíveis p obtemos a mesma desigualdade em R. Portanto, tendo em conta o teorema 1.7, o teorema 1.21 de facto diz que, para R DIP, as desigualdades (1.37) (assim como igualdade a menos de multiplicação por unidades, no caso $I = J = K = \{1,\dots,n\}$) definem a solução do problema dos fatores invariantes do produto de matrizes.

Usando uma estratégia inspirada na demonstração do teorema sobre os valores próprios das somas de matrizes hermíticas, Caldeira e Queiró obtiveram o seguinte resultado:

Teorema 1.52. *[3] Dados I, J, K subconjuntos de $\{1,\dots,n\}$ com $\#I = \#J = \#K$ tais que a desigualdade (1.37) é verdadeira em DIPs. Então é verdadeira em DDEs.*

Observação 1.53. Ao contrário do caso dos DIPs, não está confirmado se estas desigualdades consistem na solução completa do problema.

Notamos que para qualquer R domínio de integridade comutativo de MDC (mesmo não sendo DDE), para uma matriz A sobre R, definimos $d_i(A)$ como em (1.1). Temos que $d_i(A) \mid d_{i+1}(A)$. Então definimos o i-ésimo fator invariante como $\alpha_i = c$ tal que $d_i(A) = c \cdot d_{i-1}(A)$, com $d_0(A) = 1$.

Voltando ao problema de encontrar as desigualdades tipo (1.37) válidas, temos um resultado positivo importante:

Teorema 1.54. *[3] Sejam I, J, K subconjuntos de $\{1,\dots,n\}$ com $\#I = \#J = \#K$ tais que a desigualdade (1.37) é verdadeira em DDEs comutativos. Então é verdadeira em domínios de integridade comutativos de MDC.*

1.3 Fatores invariantes da soma

Consideremos agora o problema da secção 1.1 mas com $C = A + B$. Ao contrário do caso do produto, este problema não foi resolvido completamente. Conhecem-se alguns resultados relacionados. Nesta secção consideramos os elementos na diagonal da forma normal de Smith, incluindo os zeros, como sendo os fatores invariantes.

Teorema 1.55. *[19, 29] Seja R um DDE. Sejam $A, B \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $(\beta_i)_{i\in\mathbb{N}}$ respetivamente; sejam $(\gamma_i)_{i\in\mathbb{N}}$ os fatores invariantes de $C := A + B$. Então:*

$$\begin{aligned} &\operatorname{mdc}(\alpha_i, \beta_j) \mid \gamma_{i+j-1} \\ &\operatorname{mdc}(\alpha_i, \gamma_j) \mid \beta_{i+j-1} \\ &\operatorname{mdc}(\gamma_i, \beta_j) \mid \alpha_{i+j-1} \end{aligned} \tag{1.38}$$

As últimas duas igualdades obtém-se a partir da primeira com $B = C - A$ e $A = C - B$.

Para $A \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $\delta \in R$, denotamos $u_\delta(A) := \#\{i \in \{1, 2, \ldots, n\} : \alpha_i \mid \delta\}$, e $r_\delta(A) := \#\{i \in \{1, 2, \ldots, n\} : \delta \mid \alpha_i\}$.

Teorema 1.56. *[24] Seja R um DIP. Sejam $A, B \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $(\beta_i)_{i\in\mathbb{N}}$ respetivamente. Sejam $\delta \in R$, $k \in \{1, \ldots, \min\{m, n\}\}$. Se $k \neq m$ ou $k \neq n$, são equivalentes:*

(a) $\operatorname{mdc}(\alpha_1, \beta_k), \ldots, \operatorname{mdc}(\alpha_k, \beta_1)$ *dividem* δ

(b) *Existem $A', B' \in M_{m,n}(R)$ equivalentes a A e B respetivamente tais que $u_\delta(A' + B') \geq k$*

Teorema 1.57. *[24] Seja R um DIP. Sejam $A, B \in M_n(R)$ com fatores invariantes $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ respetivamente. São equivalentes:*

(a) $\operatorname{mdc}(\alpha_1, \beta_n), \ldots, \operatorname{mdc}(\alpha_n, \beta_1)$ *são unidades e existem $a, b, u, v \in R$ em que u e v são unidades tais que:*

$$a\alpha_1 + u\beta_1 \cdots \beta_n = 1; b\beta_1 + v\alpha_1 \cdots \alpha_n = 1 \tag{1.39}$$

(b) *Existem $A', B' \in M_n(R)$ equivalentes a A e B respetivamente tais que $A' + B' = I$*

Teorema 1.58. *[24] Seja R um DIP. Sejam $A, B \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $(\beta_i)_{i\in\mathbb{N}}$ respetivamente; sejam $\delta \in R$, $k \in \{1, \ldots, \min\{m, n\}\}$. Se $k \neq m$ ou $k \neq n$ ou $\delta = 0$, são equivalentes:*

(a) $\operatorname{mdc}(\alpha_i, \delta) \mid \beta_{i+n-k}$ *e* $\operatorname{mdc}(\beta_i, \delta) \mid \alpha_{i+n-k}$

(b) *Existem $A', B' \in M_{m,n}(R)$ equivalentes a A e B respetivamente tais que $r_\delta(A' + B') \geq k$*

Note-se que, tomando $\delta = 0$, temos $r_0(A) = n - \operatorname{car}(A)$, obtendo o seguinte:

Corolário 1.59. *[25] Seja R um DIP. Sejam $A, B \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $(\beta_i)_{i\in\mathbb{N}}$, $1 \leq k \leq \min\{m, n\}$. São equivalentes:*

(a) $\alpha_i \mid \beta_{i+k}$ *e* $\beta_i \mid \alpha_{i+k}$

(b) *Existem $A', B' \in M_{m,n}(R)$ equivalentes a A e B respetivamente tais que $\operatorname{car}(A' + B') \leq k$*

Teorema 1.60. *[25] Seja R um DIP. Sejam $A, B \in M_{m,n}(R)$ com $m + n > 2$ e fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $(\beta_i)_{i\in\mathbb{N}}$ respetivamente, $1 \leq k \leq \min\{m, n\}$. São equivalentes:*

(a) $\alpha_i \mid \beta_{i+k}$, $\beta_i \mid \alpha_{i+k}$ *e* $k \leq \operatorname{car}(\operatorname{diag}(\alpha_1, \ldots, \alpha_n)) + \operatorname{car}(\operatorname{diag}(\beta_1, \ldots, \beta_n))$

(b) *Existem* $A', B' \in M_{m,n}(R)$ *equivalentes a* A *e* B *respetivamente tais que* $\operatorname{car}(A' + B') = k$

Observação 1.61. Em qualquer dos 4 teoremas (e o corolário) anteriores, $A' + B' = XAY + ZBW$ para $X, Y, Z, W \in GL_n(R)$ e é equivalente a $Z^{-1}XAYW^{-1} + B$. Pelo que (b) no teorema 1.56 é equivalente a:

(b') Existe $A' \in M_{m,n}(R)$ equivalente a A tal que $u_\delta(A' + B) \geq r$

Análogamente para os outros teoremas.

Note-se que $\det(A) = u\alpha_1 \cdots \alpha_n$, onde u é uma unidade. É, então, natural analisar o determinante. Escolhemos os fatores invariantes de modo que $u = 1$.

Aqui, $a \equiv b \pmod{m}$ significa $m \mid a - b$.

Teorema 1.62. [4] *Seja* R *um DDE. Sejam* $A, B \in M_n(R)$ *com fatores invariantes* $\alpha_1, \ldots, \alpha_n$ *e* $\beta_1, \ldots, \beta_n$, *e sejam* $\gamma_1, \cdots \gamma_n$ *os fatores invariantes de* $C := A + B$. *Sejam*

$$\begin{aligned} \delta &:= \operatorname{mdc}\{\alpha_1 \cdots \alpha_k \beta_1 \cdots \beta_{n-k} : 1 \leq k \leq n-1\} \\ \theta &:= \operatorname{mdc}\{\alpha_1 \cdots \alpha_k \gamma_1 \cdots \gamma_{n-k} : 1 \leq k \leq n-1\} \\ \eta &:= \operatorname{mdc}\{\beta_1 \cdots \beta_k \gamma_1 \cdots \gamma_{n-k} : 1 \leq k \leq n-1\} \end{aligned} \tag{1.40}$$

Temos:

$$\begin{aligned} &\textstyle\prod_{i=1}^n \gamma_i \equiv \prod_{i=1}^n \alpha_i + \prod_{i=1}^n \beta_i \pmod{\delta} \\ &\textstyle\prod_{i=1}^n \beta_i \equiv (-1)^n \prod_{i=1}^n \alpha_i + \prod_{i=1}^n \gamma_i \pmod{\theta} \\ &\textstyle\prod_{i=1}^n \alpha_i \equiv (-1)^n \prod_{i=1}^n \beta_i + \prod_{i=1}^n \gamma_i \pmod{\eta} \end{aligned} \tag{1.41}$$

Teorema 1.63. [4] *Seja* R *um DDE. Sejam* $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in R$ *tais que* $\alpha_i \mid \alpha_{i+1}$, $\beta_i \mid \beta_{i+1}$. *Definimos* δ *como no teorema 1.62. Existem* $A, B \in M_n(R)$ *com fatores invariantes* $\alpha_1, \ldots, \alpha_n$ *e* $\beta_1, \ldots, \beta_n$ *respetivamente e tais que* $\det(A + B) = x$ *se e só se:*

$$x \equiv \prod_{i=1}^n \alpha_i + \prod_{i=1}^n \beta_i \pmod{\delta} \tag{1.42}$$

Teorema 1.64. [4] *Seja* R *um DDE. Sejam* $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n, \gamma_1, \ldots, \gamma_n \in R$ *com* $\alpha_i \mid \alpha_{i+1}, \beta_i \mid \beta_{i+1}, \gamma_i \mid \gamma_{i+1}$ *tais que satisfazem as igualdades (1.41). Então:*

$$\begin{aligned} &\textstyle\prod_{i=1}^n \alpha_i \equiv (-1)^n \prod_{i=1}^n \beta_i \pmod{\gamma} \\ &\textstyle\prod_{i=1}^n \beta_i \equiv \prod_{i=1}^n \gamma_i \pmod{\alpha} \\ &\textstyle\prod_{i=1}^n \gamma_i \equiv \prod_{i=1}^n \alpha_i \pmod{\beta} \end{aligned} \tag{1.43}$$

onde $\alpha = \alpha_1 \prod_{i=1}^{n-1} \operatorname{mdc}(\alpha_1, \beta_i)$, $\beta = \beta_1 \prod_{i=1}^{n-1} \operatorname{mdc}(\beta_1, \gamma_i)$, $\gamma = \gamma_1 \prod_{i=1}^{n-1} \operatorname{mdc}(\gamma_1, \alpha_i)$

Estas igualdades foram primeiro dadas por Sá [21] como condições necessárias. O teorema anterior diz que são, de facto, consequências lógicas de (1.41).

O recíproco, isto é, se (1.43) implicam (1.41), é um problema em aberto [4].

Thompson tentara dar a solução completa, chegando à seguinte condição necessária:

Teorema 1.65. *[30, 4] Seja R um DIP. Sejam $A, B \in M_n(R)$ com fatores invariantes $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$, e sejam $\gamma_1, \cdots \gamma_n$ os fatores invariantes de $C := A + B$. Então temos:*

$$\begin{array}{l} \prod_{i=1}^n \alpha_i \equiv (-1)^n \prod_{i=1}^n \beta_i \pmod{\gamma_1 \omega^{n-1}} \\ \prod_{i=1}^n \beta_i \equiv \prod_{i=1}^n \gamma_i \pmod{\alpha_1 \omega^{n-1}} \\ \prod_{i=1}^n \gamma_i \equiv \prod_{i=1}^n \alpha_i \pmod{\beta_1 \omega^{n-1}} \end{array} \tag{1.44}$$

onde $\omega := \mathrm{mdc}(\alpha_1, \beta_1, \gamma_1)$.

Thompson conjeturou que (1.44), em conjunto com (1.38), definem a solução do problema. Sá [21] provou esta conjetura falsa no caso de DDEs, ao dar as condições (1.43) e mostrando que não são consequência das dadas por Thompson e de (1.38). De facto, também mostrou que (1.44) são consequência de (1.43) e (1.38)

Todas as condições necessárias apresentadas são consequência de (1.38) e (1.41), pelo que estas condições são candidatas razoáveis a condições suficientes. De facto, Caldeira e Queiró contribuíram para esta investigação conjeturando que são condições suficientes. Eliminando a hipótese que $\det(A) = \alpha_1 \cdots \alpha_n$, obtemos:

Conjetura. *[4] Seja R um DDE. Sejam $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$, $\gamma_1, \ldots, \gamma_n \in R$ com $\alpha_i \mid \alpha_{i+1}$, $\beta_i \mid \beta_{i+1}$, $\gamma_i \mid \gamma_{i+1}$. Sejam δ, θ, η como no teorema 1.62. Existem $A, B, C \in M_n(R)$ com fatores invariantes sobre R $\alpha_1, \ldots, \alpha_n$; $\beta_1, \ldots, \beta_n$; $\gamma_1, \ldots, \gamma_n$ respetivamente, tais que $C = A + B$ se e só se (1.38) forem satisfeitas e existirem unidades u e v tais que:*

$$\begin{array}{l} \prod_{i=1}^n \gamma_i \equiv u \prod_{i=1}^n \alpha_i + v \prod_{i=1}^n \beta_i \pmod{\delta} \\ \prod_{i=1}^n \gamma_i \equiv u \prod_{i=1}^n \alpha_i + (-1)^{n+1} v \prod_{i=1}^n \beta_i \pmod{\theta} \\ \prod_{i=1}^n \gamma_i \equiv (-1)^{n+1} u \prod_{i=1}^n \alpha_i + v \prod_{i=1}^n \beta_i \pmod{\eta} \end{array} \tag{1.45}$$

Capítulo 2

Algumas generalizações

Neste capítulo, iremos generalizar alguns teoremas apresentados no capítulo anterior para anéis não comutativos e com existência de divisores de zero. Importa, portanto, introduzir a noção de fator invariante e suas propriedades em anéis não comutativos, assim como conceitos relacionados.

2.1 Introdução aos anéis não comutativos

Consideremos então um anel R qualquer.

De acordo com a terminologia de, por exemplo, [15]:

Definição 2.1. Um anel R diz-se um *domínio* se $R \neq 0$ e $ab = 0$ implicar $a = 0$ ou $b = 0$, isto é, não existirem divisores de zero esquerdos nem direitos.

Necessitamos de uma relação de divisão alternativa que implica as divisões esquerda e direita usuais (dadas pela ordem nos ideais esquerdos e direitos respetivamente), e equivalente a estas no caso comutativo.

Assim, definimos a divisão total como:

Definição 2.2 (Divisão Total)**.** [10, Pág. 40] Sejam $a, b \in R$. *a divide totalmente b* ($a \mid b$) se

$$RbR \subseteq aR \cap Ra \tag{2.1}$$

Teorema 2.3. *[10, Pág. 40] Sejam $a, b \in R$. a divide totalmente b se e só se existir um ideal bilateral I de R, tal que $bR \subseteq I \subseteq aR$ (ou, equivalentemente, $Rb \subseteq I \subseteq Ra$).*

Satisfaz todas as propriedades usuais da divisibilidade, com exceção de que um elemento não necessariamente se divide a si próprio. Temos $a \mid a$ se e só se $aR = Ra$ (neste caso aR é um ideal bilateral).

Assim definimos os fatores invariantes e forma normal de Smith de maneira semelhante, com a condição que α_i divide totalmente α_{i+1}.

Definição 2.4 (Anel de divisores elementares)**.** [12] Um anel R diz-se um *anel de divisores elementares (ADE)* se toda a matriz A sobre R tiver forma normal de Smith, isto é, for equivalente a uma matriz diagonal

$$D = \begin{bmatrix} \operatorname{diag}(\alpha_1, \ldots, \alpha_k) & 0 \\ 0 & 0 \end{bmatrix}$$

onde $\alpha_i \neq 0$, $\alpha_i \mid \alpha_{i+1}$ para $1 \leq i \leq k-1$.

Se R é adicionalmente um domínio, podemos referir R como *domínio de divisores elementares (DDE)*, como já se definiu atrás.

Definição 2.5. Dado um anel qualquer R, o *radical de Jacobson* $\operatorname{Rad}(R)$ é a interseção de todos os ideais esquerdos maximais (ou equivalentemente, ideais direitos maximais) de R.

Teorema 2.6. *[15] Seja R um anel qualquer. $x \in \operatorname{Rad}(R)$ se e só se para todo $r \in R$, $1 - rx$ for invertível à esquerda.*

Teorema 2.7. *[12, Lema 2.1] Seja R um anel tal que todos os divisores direitos de zero estão em $\operatorname{Rad}(R)$. Então, dados $x, y \in R$, se $xR = yR$ então existe unidade u tal que $x = yu$.*

O teorema 1.49 que dá uma condição necessária e suficiente para ser um ADE no caso comutativo também se aplica quando todos os divisores de zero estão em $\operatorname{Rad}(R)$.

Dois elementos $a, b \in R$ dizem-se *associados* (denotamos $a \sim b$) se $a \mid b$ e $b \mid a$, ou equivalentemente, se $aR = bR = Ra = Rb = RaR = RbR$. Coincide com a definição dada anteriormente ($a = bu$ para u unidade) em domínios de integridade comutativos, como mostra o teorema 2.7.

No caso não comutativo, não temos unicidade dos fatores invariantes a menos de associados.

Definição 2.8. Um anel R diz-se um *anel de Bézout* se todo o ideal esquerdo ou direito finitamente gerado for principal.

Definição 2.9. Um anel R é um *anel de Hermite direito* se todas as matrizes 1×2 tiverem redução diagonal, isto é, para todos $a, b \in R$ existe $U \in GL_2(R)$ tal que $\begin{bmatrix} a & b \end{bmatrix} U = \begin{bmatrix} d & 0 \end{bmatrix}$.

Definição 2.10. Um anel R é um *anel de Hermite esquerdo* se todas as matrizes 2×1 tiverem redução diagonal, isto é, para todos $a, b \in R$ existe $U \in GL_2(R)$ tal que $U \begin{bmatrix} a & b \end{bmatrix}^T = \begin{bmatrix} d & 0 \end{bmatrix}^T$.

Definição 2.11. Um anel R é um *anel de Hermite* se for Hermite esquerdo e Hermite direito.

Teorema 2.12. *[12, Teorema 3.5] Sejam R um anel de Hermite direito, $A \in M_{m,n}(R)$. Então existe $U \in GL_n(R)$ tal que AU tem entradas nulas acima da diagonal que inicia no canto superior esquerdo.*

Também podemos escolher $U \in GL_n(R)$ tal que AU tem entradas nulas debaixo da diagonal que inicia no canto inferior direito. No caso de anéis de Hermite esquerdos, UA (com $U \in GL_m(R)$) pode ter entradas nulas debaixo da diagonal que inicia no canto superior esquerdo ou entradas nulas acima da diagonal que inicia no canto inferior direito.

Teorema 2.13. *[12, Pág. 465] Seja R um anel de Hermite. Então é um anel de Bézout.*

Teorema 2.14. *[12, Teorema 3.1] Seja R um anel tal que:*

(a) *todos os seus divisores de zero (esquerdos e direitos) estão em* $\mathrm{Rad}(R)$

(b) *é um anel de Bézout*

(c) *a intersecção de quaisquer dois ideais principais direitos for principal*

(d) *para qualquer $A \in M_2(R)$ com inversa esquerda ou direita, $A \in GL_2(R)$.*

Então R é um anel de Hermite direito.

Corolário 2.15. *[12, Teorema 3.2] Seja R um anel comutativo de Bézout cujos divisores de zero estão em* $\mathrm{Rad}(R)$*. Então R é um anel de Hermite.*

Teorema 2.16. *[12, Teorema 3.4] Seja R um domínio. Então R é um anel de Hermite se e só se for um anel de Bézout e a intersecção de quaisquer dois ideais principais esquerdos ou direitos for principal.*

Kaplansky deu uma observação simples e útil em relação aos ADE:

Teorema 2.17. *[12, Teorema 5.1] Um anel R é um ADE se e só se todas as matrizes 1×2, 2×1 e 2×2 tiverem forma normal de Smith.*

Teorema 2.18. *[12] Um domínio R é um DDE se e só se todas as matrizes 2×2 tiverem forma normal de Smith.*

Definição 2.19. Um anel R diz-se *duo* se todos os seus ideais esquerdos e ideais direitos forem bilaterais.

Teorema 2.20. *Um anel R é duo se e só se*

$$aR = Ra \, \forall a \in R \tag{2.2}$$

Ou seja, um anel é duo exatamente quando todos os seus elementos se dividem a si próprios. Isto implica que a associatividade é uma relação de equivalência. Neste caso, escolhemos um representante em cada classe de equivalência, sendo a classe das unidades representada por 1. Se X for um subconjunto de R e existir um máximo divisor comum d de X, então os máximos divisores comuns de X são todos os elementos associados a d e denotamos o representante desta classe por $\mathrm{mdc}(X)$. Analogamente, $\mathrm{mmc}(X)$ denota o representante dos mínimos múltiplos comuns de X se existirem.

Note-se que num anel duo, a divisão total é equivalente às divisões esquerda e direita.

A próxima definição leva-nos a outra condição suficiente para um anel ser ADE:

Definição 2.21. [9, 12] Um anel duo R diz-se um *anel adequado* se for um anel de Bézout e se, dados $a, c \in R$ com $a \neq 0$, existirem r, s tais que $a = rs$, $\mathrm{mdc}(r, c) = 1$ e $\mathrm{mdc}(s', c) \neq 1$ para qualquer s' divisor de s exceto unidades.

Teorema 2.22. *[12, Teorema 5.3] [9] Seja R um anel comutativo cujos divisores de zero estão em* $\mathrm{Rad}(R)$*. Se R for adequado, R é um ADE.*

O teorema 1.1 das desigualdades de entrelaçamento pode ser estendido para ADEs duo:

Teorema 2.23 (Desigualdades de Entrelaçamento)**.** *[6] Sejam R um ADE duo, $A \in M_{m,n}(R)$ com fatores invariantes $(\alpha_i)_{i\in\mathbb{N}}$ e $B \in M_{p,q}(R)$ com $p \leq m, q \leq n, m+n-(p+q) \geq 1$ e cujos fatores invariantes são $(\beta_i)_{i\in\mathbb{N}}$. Existe A' equivalente a A tal que contém B como submatriz se e só se tivermos (1.2), isto é, para qualquer i:*

$$\alpha_i \mid \beta_i \mid \alpha_{i+m+n-p-q}$$

Observação 2.24. No caso $p+q = m+n$ a hipótese reduz-se a B ser equivalente a A e a desigualdade (1.2) reduz-se a $\alpha_i \mid \beta_i \mid \alpha_i$ (isto é, $\alpha_i \sim \beta_i$), que é uma condição necessária [6], mas não foi mostrada ser suficiente. É suficiente no caso em que todos os divisores de zero estão em $\mathrm{Rad}(R)$, por consequência do teorema 2.7.

A seguir, mostramos uma propriedade notória dos DDEs duo.

Lema 2.25. *[6] Sejam R qualquer anel, $A \in M_{m,n}(R), B \in M_{n,p}(R)$. Se $d \in R$ dividir todas as entradas de A então divide todas as entradas de AB.*

Corolário 2.26. *[6] Seja R qualquer anel. Sejam $A, A' \in M_{m,n}(R)$. Se A e A' forem equivalentes, então $d \in R$ divide todas as entradas de A se e só se dividir todas as entradas de A'.*

Corolário 2.27. *[6] Seja R um anel duo. Para $A \in M_{m,n}(R)$ com forma normal de Smith, um seu primeiro fator invariante é* mdc *das suas entradas.*

Demonstração. A é equivalente a

$$A' = \begin{bmatrix} \mathrm{diag}(\alpha_1, \ldots, \alpha_k) & 0 \\ 0 & 0 \end{bmatrix}$$

com $\alpha_i \mid \alpha_{i+1}$. Sendo R duo, temos que α_1 divide-se a si próprio, logo é mdc das entradas de A'. Pelo corolário 2.26, α_1 é mdc das entradas de A. □

Corolário 2.28. *Seja R um DDE duo. Então R é um anel de MDC.*

Demonstração. Para $a, b \in R$, seja $A = \mathrm{diag}(a, b)$. Sendo R um DDE, A tem forma normal de Smith. A conclusão segue do corolário 2.27. □

2.2 Algumas generalizações

Nesta secção, estendemos alguns dos teoremas apresentados para classes de anéis maiores, nomeadamente, ADEs duo.

2.2.1 Condições suficientes para anéis de Hermite e ADEs em anéis duo

Esta subsecção tem como objetivo generalizar dois teoremas de Kaplansky [12], apresentando as seguintes demonstrações, de acordo com o estudo realizado em colaboração com o Prof. Fernando Silva.

Lema 2.29. *Sejam R um anel duo, $m, a, b \in R$. Se $m \mid ab$ e $Ra + Rm = R$, então $m \mid b$.*

Demonstração. Suponhamos que $1 = ra + sm$ e $ab = xm$. Então $ra = 1 - sm$, $(1 - sm)b = rab = rxm$, $b = rxm + smb \in Rm$, isto é $m \mid b$. □

Lema 2.30. *Sejam R um anel duo, $a, b \in R$ com $Ra + Rb = R$. Então ab é* mmc *de $\{a, b\}$.*

Demonstração. ab é certamente múltiplo de a e de b. Seja $x = ac = bc'$ para alguns $c, c' \in R$. Então $b \mid ac$. Pelo lema anterior, $b \mid c$. Logo $ab \mid ac = x$. □

Lema 2.31. *Seja R um anel duo tal que os divisores de 0 estão em* $\mathrm{Rad}(R)$. *Sejam $a, b \in R$. Então temos a e b associados se e só se existir $u \in R$ unidade tal que $b = au$ se e só se existir $u' \in R$ unidade tal que $b = u'a$.*

Demonstração. É consequência do teorema 2.7 tendo em conta que, sendo R duo, a e b são associados se e só se $Ra = Rb$ (se e só se $aR = bR$). Os recíprocos são triviais. □

Lema 2.32. *Seja R um anel de Bézout duo. Sejam $d, a, b \in R$. Então $dR = aR + bR$ se e só se d for* mdc *de $\{a, b\}$. Logo existe* mdc *de qualquer par de elementos de R (R é um anel de MDC).*

Demonstração. ($\Rightarrow$) Assumimos que $dR = aR + bR$. Temos $d \mid a$ e $d \mid b$. Assumimos que $d' \mid a$ e $d' \mid b$. Então $dR = aR + bR \subseteq d'R$ e $d' \mid d$. Logo d é mdc de $\{a, b\}$.

($\Leftarrow$) Por hipótese, existe $c \in R$ tal que $cR = aR + bR$. Pelo parágrafo anterior, c é mdc de $\{a, b\}$. Assumimos que d é mdc de $\{a, b\}$. Então $d \mid c$, $c \mid d$ e $dR = cR = aR + bR$. □

Lema 2.33. *Seja R um anel de Bézout duo tal que os divisores de 0 estão em* $\mathrm{Rad}(R)$. *Sejam $a, b \in R$ com $a \neq 0$ ou $b \neq 0$. Suponhamos $dR = aR + bR$ e $d = ap + bq$ onde $d, p, q \in R$. Então* $\mathrm{mdc}(p, q) = 1$.

Demonstração. Seja c um mdc de $\{p, q\}$. Então $p = p'c$ e $q = q'c$ para certos $p', q' \in R$. Então $d = d'c$ onde $d' = ap' + bq' \in aR + bR = dR$. Então d e d' são associados. Então $d' = du$ para $u \in R$ unidade. Então $d(1 - uc) = 0$. Note-se que $d \neq 0$. Então, $1 - uc \in \mathrm{Rad}(R)$. Pelo teorema 2.6, uc é uma unidade, pelo que $R = Ruc = Rc = cR$, isto é, c é uma unidade. Logo $\mathrm{mdc}(p, q) = 1$. □

Lema 2.34. *Seja R um anel de Bézout duo cujos divisores de 0 estão em* $\mathrm{Rad}(R)$. *Se* $\mathrm{mdc}(p, q) = 1$, *então existe uma matriz 2×2 invertível cuja primeira coluna é $\begin{bmatrix} p & q \end{bmatrix}^T$ (e também existe uma matriz 2×2 invertível cuja primeira linha é $\begin{bmatrix} p & q \end{bmatrix}$).*

Demonstração. Se $1 = 0$, o lema é trivial. Supomos $1 \neq 0$. Supomos que $\text{mdc}(p, q) = 1$. Então $p \neq 0$ ou $q \neq 0$. Supomos que $q \neq 0$. O outro caso é análogo. Pelo lema 2.32, $R = pR + qR = Rp + Rq$. Logo $1 = rp + sq$ para certos $r, s \in R$. Temos $qp = p'q$ para certo $p' \in R$.

Mostramos que $\text{mdc}(p', q) = 1$. Seja a um mdc de $\{p', q\}$. Como $R = pR + qR$ e $aR = p'R + qR$, $qR = qpR + q^2R = (p'R + qR)q = aRq = Raq$. Então $q = xaq$ para certos $x \in R$. Como $q \neq 0$, $1 - xa \in \text{Rad}(R)$. Pelo teorema 2.6, xa é uma unidade. Como $xa \in Ra = aR$, existe $y \in R$ tal que $xa = ay$. Como $((xa)^{-1}x)a = 1 = a(y(xa)^{-1})$, a é uma unidade. Logo $\text{mdc}(p', q) = 1$.

Então $R = p'R + qR$ e $1 = p'r' + qs'$ para certos $r', s' \in R$. Seja

$$U = \begin{bmatrix} p & s' \\ q & -r' \end{bmatrix}. \text{ Então } \begin{bmatrix} r & s \\ q & -p' \end{bmatrix} U = \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}, \text{ onde } z = rs' - sr'.$$

Multiplicando à esquerda ambos os lados da última igualdade por: $\begin{bmatrix} 1 & -z \\ 0 & 1 \end{bmatrix}$, deduzimos que U tem inversa esquerda. A seguir mostramos que U tem também inversa direita. Existe $r'' \in R$ tal que $r'q = qr''$. Então $p'r'q = p'qr'' = qpr''$. Então $q = (p'r' + qs')q = q(pr'' + s'q)$. Como $q \neq 0$, $1 - (pr'' + s'q) \in \text{Rad}(R)$. Pelo teorema 2.6, $u := pr'' + s'q$ é uma unidade. Existe $p'' \in R$ tal que $p'r' = r'p''$. Então

$$U \begin{bmatrix} r''u^{-1} & s' \\ qu^{-1} & -p'' \end{bmatrix} = \begin{bmatrix} 1 & w \\ 0 & 1 \end{bmatrix}, \text{ onde } w = ps' - s'p''.$$

Multiplicando à direita ambos os lados da última igualdade por: $\begin{bmatrix} 1 & -w \\ 0 & 1 \end{bmatrix}$, deduzimos que U tem inversa direita. Logo U é invertível. □

O seguinte teorema generaliza o teorema 2.14.

Teorema 2.35. *Seja R um anel de Bézout duo cujos divisores de 0 estão em $\text{Rad}(R)$. Então R é um anel de Hermite.*

Demonstração. Sejam $a, b \in R$. Mostramos que ambas as matrizes $\begin{bmatrix} a & b \end{bmatrix}$ e $\begin{bmatrix} a & b \end{bmatrix}^T$ têm reduções diagonais. É trivial se $a = b = 0$. Supõe-se que $a \neq 0$ ou $b \neq 0$. Seja c um mdc de $\{a, b\}$. Então $c = ap + bq$ onde $\text{mdc}(p, q) = 1$. Pelo lema anterior, existe uma matriz invertível U cuja primeira coluna é $\begin{bmatrix} p & q \end{bmatrix}^T$. Então $\begin{bmatrix} a & b \end{bmatrix} U = \begin{bmatrix} c & cx \end{bmatrix}$ para algum $x \in R$. Então

$$\begin{bmatrix} a & b \end{bmatrix} U \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c & 0 \end{bmatrix} \text{ é a redução diagonal de } \begin{bmatrix} a & b \end{bmatrix}.$$

Analogamente provamos que $\begin{bmatrix} a & b \end{bmatrix}^T$ tem redução diagonal. □

Os resultados anteriores, assim como o lema que apresentaremos a seguir, contribuem para generalização do teorema 1.49:

Lema 2.36. *Sejam R um domínio duo, $d \in R\backslash\{0\}$, $X \in GL_n(R)$. Seja $X' \in M_n(R)$ tal que $Xd = dX'$ (existe pois R é duo). Então $X' \in GL_n(R)$.*

Demonstração. Sejam $Y := X^{-1}$ e Y' tal que $Yd = dY'$. Temos $dI = XYd = XdY' = dX'Y'$, logo $I = X'Y'$. Analogamente, $I = Y'X'$. Portanto, X' é invertível. □

Teorema 2.37. *Seja R um domínio duo. R é um DDE se e só se:*

(a) *For um anel de Bézout.*

(b) *Para $a, b, c \in R$ tais que $\mathrm{mdc}(a, b, c) = 1$, existirem $p, q \in R$ tais que $\mathrm{mdc}(pa, pb + qc) = 1$.*

Demonstração. Assumimos que R é um DDE. Pelo teorema 2.13, como R é um anel de Hermite, temos (a). Agora seja

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \tag{2.3}$$

tal que $\mathrm{mdc}(a, b, c) = 1$, e assumimos que $P, Q \in GL_2(R)$ são tais que PAQ é uma forma normal de Smith de A. Pelo corolário 2.27, a entrada do canto superior esquerdo de PAQ é uma unidade u. Suponhamos que a primeira linha de P é $\begin{bmatrix} p & q \end{bmatrix}$ e que a primeira coluna de Q é $\begin{bmatrix} x & y \end{bmatrix}^T$. Então $u = (pa)x + (pb + qc)y$, logo $\mathrm{mdc}(pa, pb + qc) = 1$ e temos (b).

Agora assumimos que R satisfaz (a) e (b). Pelo teorema 2.18, basta provar que qualquer matriz 2×2 tem forma normal de Smith. Pelo teorema 2.35, R é um anel de Hermite. Portanto, dada uma tal matriz, temos que é equivalente a uma matriz como A acima. Seja $d := \mathrm{mdc}(a, b, c)$. Se $d = 0$, $A = 0$. Para $d \neq 0$, seja A' tal que $A = A'd$. Sejam $X, Y \in GL_2(R)$ tais que $A' = XDY$, onde D é uma forma normal de Smith de A'. Pelo lema 2.36, Y' tal que $Yd = dY'$ é invertível. Então, $A = A'd = XDYd = XDdY'$, sendo Dd uma forma normal de Smith de A. Basta então provar que A' tem redução diagonal. Sejam a', b', c' as entradas não nulas de A' e $d' := \mathrm{mdc}(a', b', c')$. Temos que $d'd$ divide a, b e c, pelo que $d' = 1$. Tomamos então p, q tais que $\mathrm{mdc}(pa', pb' + qc') = 1$ dados por (b). Observe-se que $\mathrm{mdc}(p, q) = 1$. Pelo lema 2.34 existe $P \in GL_2(R)$ com primeira linha $\begin{bmatrix} p & q \end{bmatrix}$. A primeira linha de PA' é então $\begin{bmatrix} pa' & pb' + qc' \end{bmatrix}$. Sendo R Hermite, esta é equivalente a uma matriz com primeira linha $\begin{bmatrix} 1 & 0 \end{bmatrix}$. Multiplicando à esquerda por uma matriz elementar para eliminar a entrada inferior esquerda, obtemos a forma desejada. □

De acordo com o teorema anterior, podemos generalizar o teorema 2.22 para domínios duo.

2.2.2 Caraterização alternativa de fatores invariantes em ADEs duo

Iremos generalizar para ADEs duo os teoremas de Queiró em [19] apresentados na secção 1.2, nomeadamente a caraterização dos fatores invariantes, assim como a sua demonstração de (1.38).

Sendo envolvida a noção de caraterística de matriz, por diante, car significa caraterística interna e denotamos a caraterística interna de uma matriz A por $\mathrm{car}(A)$.

Mostramos que a noção de caraterística interna é simplificada no caso de existência de redução diagonal.

Teorema 2.38. *Seja R um ADE duo. A caraterística interna de $A \in M_{m,n}(R)$ é igual ao número r de fatores invariantes não nulos em qualquer redução diagonal de A.*

Demonstração. Seja $A = UCV$, onde U, V são invertíveis.

$$C = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}, \quad D = \operatorname{diag}(d_1, \ldots, d_r), \quad d_i \mid d_{i+1} \quad \text{e} \quad d_i \neq 0.$$

Seja W a submatriz $m \times r$ de U correspondendo às primeiras r colunas. Seja X a submatriz $r \times n$ de V correspondendo às primeiras r linhas. Então

$$A = U \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} V = U \begin{bmatrix} \begin{bmatrix} D & 0 \end{bmatrix} V \\ 0 \end{bmatrix} = U \begin{bmatrix} DX \\ 0 \end{bmatrix} = WDX$$

isto é, $A = W(DX)$, o que mostra que $\operatorname{car}(A) \leq r$.

Seja $s = \operatorname{car}(A)$ e assumimos que $A = LK$ onde $L \in M_{m,s}(R)$ e $K \in M_{s,n}(R)$. Como R é um anel de Hermite, pelo teorema 2.12, existem matrizes $Y \in GL_m(R)$ e $Z \in GL_n(R)$ tais que YL tem as últimas $m - s$ linhas nulas e KZ tem as últimas $n - s$ colunas nulas. Então A é equivalente a

$$YAZ = \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} \quad \text{onde} \quad S \in M_s(R).$$

Segue-se que A tem redução diagonal com no máximo s fatores invariantes não nulos. Logo $s = r$. □

Primeiro, generalizamos o corolário 1.59:

Teorema 2.39. *Seja R um ADE duo. Sejam $A, B \in M_{m,n}(R)$ e seja $r \in \mathbb{N}$. Supomos que A e B têm reduções diagonais com fatores invariantes $(a_i)_{i\in\mathbb{N}}$ e $(b_i)_{i\in\mathbb{N}}$, respetivamente. Existem $A', B' \in M_{m,n}(R)$ equivalentes a A, B, respetivamente, tais que $\operatorname{car}(A' - B') \leq r$ se e só se, para cada i, $a_i \mid b_{i+r}$ e $b_i \mid a_{i+r}$.*

Demonstração. ($\Rightarrow$) Seja $C := A' - B'$. Sejam U e V matrizes invertíveis tais que $D = UCV$ é redução diagonal de C. Então $UCV = A'' - B''$ onde $A'' = UA'V = \begin{bmatrix} E & G \end{bmatrix}$, $B'' = UA'V = \begin{bmatrix} F & G \end{bmatrix}$, e $G \in M_{m,n-r}(R)$. Seja $(g_i)_{i\in\mathbb{N}}$ uma cadeia de fatores invariantes de G. Pelo teorema 2.23, $a_i \mid g_i \mid a_{i+r}$ e $b_i \mid g_i \mid b_{i+r}$. Então $a_i \mid b_{i+r}$ e $b_i \mid a_{i+r}$.

($\Leftarrow$) Para cada $i \in \mathbb{N}_0$, seja $g_i = \operatorname{mdc}(a_{i+r}, b_{i+r})$. Notamos que $g_i = 0$ para $i > \min\{m, n\} - r$. Seja $G \in M_{m,n-r}(R)$ uma matriz com fatores invariantes $(g_i)_{i\in\mathbb{N}}$. Então $a_i \mid g_i \mid a_{i+r}$ e $b_i \mid g_i \mid b_{i+r}$. Pelo teorema 2.23, A é equivalente a uma matriz $A' = \begin{bmatrix} E & G \end{bmatrix}$ e B é equivalente a uma matriz $B' = \begin{bmatrix} F & G \end{bmatrix}$. Então $A' - B' = \begin{bmatrix} E - F & 0 \end{bmatrix}$, logo $A' - B'$ tem redução diagonal com no máximo r fatores invariantes não nulos, isto é, $\operatorname{car}(A' - B') \leq r$. □

Segue-se que o teorema 1.60 generaliza-se a DDEs comutativos, pois a sua demonstração original usa o corolário 1.59 e é válida neste contexto.

Para um anel de MDC R, $A \in M_{m,n}(R)$, $A = [a_{i,j}]$, definimos $u(A) := \text{mdc}\{a_{i,j} : 1 \leq i \leq m, 1 \leq j \leq n\}$. Se R for um ADE duo, pelo corolário 2.27, $u(A)$ é associado a um primeiro fator invariante de A. Mostramos então como estender as proposições dadas por Queiró para ADEs duo:

Lema 2.40. *Seja R um anel de MDC. Sejam $A = [a_{i,j}], B = [b_{i,j}] \in M_{m,n}(R)$. Então*

$$\text{mdc}(u(A), u(B)) \mid u(A + B)$$

Demonstração. Sejam $d = u(A)$, $e = u(B)$, $g = \text{mdc}(d, e)$. Para todos i, j, $g \mid d \mid a_{i,j}$ e $g \mid e \mid b_{i,j}$. Logo $g \mid a_{i,j} + b_{i,j}$. Segue-se que $g \mid u(A + B)$. □

Lema 2.41. *Seja R um anel de MDC duo. Sejam $A = [a_{i,j}] \in M_{m,n}(R), B = [b_{i,j}] \in M_{n,p}(R)$. Então*

$$u(A)u(B) \mid u(AB)$$

Demonstração. Sejam $d = u(A)$, $e = u(B)$. Para todos i, j, k, $d \mid a_{i,k}$ e $e \mid b_{k,j}$. Então $Ra_{i,k} \subseteq Rd$ e $b_{k,j}R \subseteq eR$. Então $Ra_{i,k}b_{k,j}R \subseteq RdeR = deR = Rde$. Então $de \mid a_{i,k}b_{k,j}$. Para todo i, j, $de \mid \sum_k a_{i,k}b_{k,j}$. Logo $u(A)u(B) \mid u(AB)$. □

Corolário 2.42. *Seja R um ADE duo. Sejam $A = [a_{i,j}] \in M_{m,n}(R), U \in GL_m(R), V \in GL_n(R)$. Então $u(A) = u(UAV)$.*

Demonstração. Sendo U e V invertíveis, temos $u(U) = u(V) = 1$. Pelo lema anterior, $u(A) = u(U)u(A)u(V) \mid u(UAV)$. Analogamente, $u(UAV) \mid u(U^{-1}UAVV^{-1}) = u(A)$. Temos a igualdade pois $u(A)$ e $u(UAV)$ são representantes de uma classe de associados. □

Teorema 2.43. *Seja R um ADE duo. Seja $A \in M_{m,n}(R)$ e seja $(a_i)_{i\in\mathbb{N}}$ uma cadeia de fatores invariantes de A. Então, para cada $k \in \mathbb{N}$, a_k é um* mmc *de $\{u(A - X) : X \in M_{m,n}(R)_k\}$.*

Demonstração. Seja $X \in M_{m,n}(R)_k$. Seja $B = A - X$. Então $\text{car}(A - B) < k$. Seja $(b_i)_{i\in\mathbb{N}}$ uma cadeia de fatores invariantes de B. Pelo teorema 2.39, para cada i, $a_i \mid b_{i+k-1}$ e $b_i \mid a_{i+k-1}$. Pelo corolário 2.27, b_1 é mdc das entradas de B. Logo $u(B) \sim b_1$. Então $u(A - X) = u(B) \sim b_1 \mid a_k$.

Supomos que $m \leq n$. O outro caso é análogo.

Supomos que $k \leq m$. Existem matrizes invertíveis U e V tais que $UAV = \begin{bmatrix}\text{diag}(a_1, \ldots, a_m) & 0\end{bmatrix}$. Seja

$$X = U^{-1} \begin{bmatrix}\text{diag}(a_1, \ldots, a_{k-1}) & 0 \\ 0 & 0\end{bmatrix} V^{-1}.$$

Então $\text{car}(X) < k$. Pelo corolário 2.42, $u(A - X) = u(U(A - X)V) \sim a_k$.

Supomos que $k > m$. Então $a_k = 0$, $A \in M_{m,n}(R)_k$ e $u(A - A) = 0$.

Em ambos os casos, a_k é um mmc de $\{u(A - X) : X \in M_{m,n}(R)_k\}$. □

Lema 2.44. *Seja R um anel qualquer. Sejam $A, B \in M_{m,n}(R)$. Então* $\mathrm{car}(A+B) \leq \mathrm{car}(A) + \mathrm{car}(B)$.

Demonstração. Sejam $r = \mathrm{car}(A)$ e $s = \mathrm{car}(B)$. Sejam $L \in M_{m,r}(R)$, $K \in M_{r,n}(R)$, $S \in M_{m,s}(R)$ e $T \in M_{s,n}(R)$ tais que $A = LK$ e $B = ST$. Então:

$$A + B = \begin{bmatrix} L & S \end{bmatrix} \begin{bmatrix} K \\ T \end{bmatrix}$$

Logo $\mathrm{car}(A+B) \leq \mathrm{car}(A) + \mathrm{car}(B)$. □

Lema 2.45. *Seja R um anel qualquer. Sejam $A \in M_{m,n}(R), B \in M_{n,p}(R)$. Então* $\mathrm{car}(AB) \leq \min\{\mathrm{car}(A), \mathrm{car}(B)\}$.

Demonstração. Sejam $r = \mathrm{car}(A)$ e $s = \mathrm{car}(B)$. Sejam $L \in M_{m,r}(R)$, $K \in M_{r,n}(R)$, $S \in M_{n,s}(R)$ e $T \in M_{s,p}(R)$ tais que $A = LK$ e $B = ST$. Então $AB = L(KB) = (AS)T$. Segue-se que $\mathrm{car}(AB) \leq \min\{\mathrm{car}(A), \mathrm{car}(B)\}$. □

Teorema 2.46. [19, Corolário 1] *Seja R um ADE duo. Sejam $A, B \in M_{m,n}(R)$. Sejam $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ e $(c_i)_{i\in\mathbb{N}}$ cadeias de fatores invariantes de A, B, e $A+B$, respetivamente. Então, para todos $k, l \in \mathbb{N}$,* $\mathrm{mdc}(a_k, b_l) \mid c_{k+l-1}$.

Demonstração. (Esta é a demonstração de [19, Corolário 1].) Sejam $k, l \in \mathbb{N}$. Seja $A_k \in M_{m,n}(R)_k$ tal que $a_k \sim u(A - A_k)$. Seja $B_l \in M_{m,n}(R)_l$ tal que $b_l \sim u(B - B_l)$. Então $\mathrm{mdc}(a_k, b_l) \sim \mathrm{mdc}(u(A-A_k), u(B-B_l)) \mid u((A-A_k)+(B-B_l)) = u((A+B)-(A_k+B_l)) \mid \mathrm{mmc}\{u((A+B)-X) : X \in M_{m,n}(R)_{k+l-1}\} \sim c_{k+l-1}$. □

Teorema 2.47. [19, Corolário 2] *Seja R um ADE duo. Sejam $A \in M_{m,n}(R), B \in M_{n,p}(R)$. Sejam $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$, e $(c_i)_{i\in\mathbb{N}}$ cadeias de fatores invariantes de A, B, e AB, respetivamente. Então, para todos $k, l \in \mathbb{N}$,* $a_k b_l \mid c_{k+l-1}$.

Demonstração. (Esta é a demonstração de [19, Corolário 2].) Sejam $k, l \in \mathbb{N}$. Seja $A_k \in M_{m,n}(R)_k$ tal que $a_k \sim u(A - A_k)$. Seja $B_l \in M_{n,p}(R)_l$ tal que $b_l \sim u(B - B_l)$. Então $a_k b_l \sim u(A-A_k)u(B-B_l) \mid u((A-A_k)(B-B_l)) = u(AB - (A_k(B-B_l) + AB_l)) \mid \mathrm{mmc}\{u(AB-X) : X \in M_{m,p}(R)_{k+l-1}\} \sim c_{k+l-1}$. □

Em particular temos $a_k b_1 \mid c_k$ e $a_1 b_k \mid c_k$, o que implica $a_k \mid c_k$ e $b_k \mid c_k$, que é o teorema 1.5.

Notamos que 1.6 também se aplica em DDEs comutativos, pois a sua demonstração usa 1.5 e é válida em DDEs comutativos.

2.2.3 Forma normal de Smith de uma matriz diagonal em anéis duo

Lema 2.48. *Sejam R um anel de Bézout duo, $\delta_1, \delta_2 \in R$. Sejam α_1 um* mdc *de $\{\delta_1, \delta_2\}$, b_1 tal que $\delta_1 = b_1\alpha_1$. Então a matriz* $\mathrm{diag}(\delta_1, \delta_2)$ *tem redução diagonal* $\mathrm{diag}(\alpha_1, b_1\delta_2)$.

Demonstração. Temos que existem a_1, a_2 tais que $\alpha_1 = a_1\delta_1 + \delta_2 a_2$. Efetuamos então a seguinte sequência de operações elementares na matriz:

$$\begin{bmatrix} \delta_1 & 0 \\ 0 & \delta_2 \end{bmatrix} \to \begin{bmatrix} \delta_1 & 0 \\ a_1\delta_1 & \delta_2 \end{bmatrix} \to \begin{bmatrix} \delta_1 & 0 \\ \alpha_1 & \delta_2 \end{bmatrix} \to \begin{bmatrix} 0 & -b_1\delta_2 \\ \alpha_1 & \delta_2 \end{bmatrix} \to \begin{bmatrix} 0 & -b_1\delta_2 \\ \alpha_1 & 0 \end{bmatrix} \to \begin{bmatrix} \alpha_1 & 0 \\ 0 & b_1\delta_2 \end{bmatrix}$$

□

Teorema 2.49. *Seja R um anel duo. Todas as matrizes quadradas diagonais sobre R têm forma normal de Smith se e só se R for um anel de Bézout.*

Demonstração. ($\Leftarrow$) O caso $n = 1$ é trivial, $n = 2$ é dado pelo lema anterior. Sejam $n > 2$ e $A = \operatorname{diag}(a_1, \ldots, a_n)$. Pelo lema anterior, podemos tomar dois índices $i \neq j$, e substituir a_i por um mdc de $\{a_i, a_j\}$ e a_j por um certo múltiplo de a_j, obtendo uma matriz equivalente a A. Efetuamos esta operação repetidamente pela seguinte ordem de índices (i, j): $(1,2), (1,3), \ldots, (1,n), (2,3), \ldots, (2,n), \ldots, (n-1,n)$.

Denotamos $c_{i,j}$ o elemento de R que, ao efetuar a operação (i, j), multiplica a j-ésima entrada diagonal da matriz à esquerda. Após efetuarmos as operações em $(1,2), (1,3), \ldots, (1,n)$, a entrada superior esquerda da matriz é $\operatorname{mdc}(a_1, \ldots, a_n)$ e, para $j > 1$, a j-ésima entrada diagonal da matriz é $c_{1,j}a_j$. Após efetuarmos as operações em $(2,3) \ldots, (2,n)$, a segunda entrada é $\operatorname{mdc}(c_{1,2}a_2, \ldots, c_{1,n}a_n)$, que é um múltiplo de $\operatorname{mdc}(a_1, \ldots, a_n)$, e, para $j > 2$, a j-ésima entrada é $c_{2,j}c_{1,j}a_j$.

Seja $i \in \{2, \ldots, n-1\}$. Assumimos que efetuámos todas as operações da sequência até (i, n), obtendo na j-ésima entrada, para $j \leq i$,

$$\operatorname{mdc}(c_{j-1,j} \cdots c_{1,j}a_j, \ldots, c_{j-1,n} \cdots c_{1,n}a_n)$$

(pelo que as primeiras i entradas formam uma cadeia de divisibilidade), e para $j > i$, $c_{i,j} \cdots c_{1,j}a_j$. Efetuando as operações em $(i+1, i+2) \ldots, (i+1, n)$, a $i+1$-ésima entrada é

$$\operatorname{mdc}(c_{i,i+1} \cdots c_{1,i+1}a_{i+1}, \ldots, c_{i,n} \cdots c_{1,n}a_n)$$

que é múltiplo da i-ésima entrada; e a j-ésima entrada, para $j > i+1$, é $c_{i+1,j} \cdots c_{1,j}a_j$. Demonstrámos, por indução, que a sequência de operações de equivalência indicada resulta numa forma normal de Smith de A.

($\Rightarrow$) Em particular, para quaisquer $a, b \in R$, $\operatorname{diag}(a, b)$ tem forma normal de Smith. Pelo corolário 2.27, temos que existe mdc de $\{a, b\}$ e é combinação linear de $\{a, b\}$. Logo, R é um anel de Bézout. □

Lema 2.50. *Sejam R um domínio duo, $a, b, c \in R$, $c \neq 0$, m um* mmc *de $\{a, b\}$. Então mc é um* mmc *de $\{ac, bc\}$.*

Demonstração. Temos que mc é certamente múltiplo de ac e de bc. Seja $x = yac = zbc$ para alguns $y, z \in R$. Então $ya = zb$ e $b \mid ya$. Portanto, $ya = y'm$ para algum $y' \in R$, logo $x = y'mc$ e $mc \mid x$. □

Lema 2.51. *Sejam R um domínio de Bézout duo, $\delta_1, \delta_2 \in R$, α_1 um* mdc *de $\{\delta_1, \delta_2\}$, b_1 tal que $\delta_1 = b_1\alpha_1$. Então $b_1\delta_2$ é um* mmc *de $\{\delta_1, \delta_2\}$.*

Demonstração. Se $\delta_1 = \delta_2 = 0$, o lema é trivial. Assumimos que $\delta_1 \neq 0$ ou $\delta_2 \neq 0$. Seja b_2 tal que $\delta_2 = b_2\alpha_1$. Notemos que 1 é mdc de $\{b_1, b_2\}$. Pelo lema 2.32, $Rb_1 + Rb_2 = R$. Pelo lema 2.30, b_1b_2 é mmc de $\{b_1, b_2\}$. Logo, pelo lema 2.50, $b_1b_2\alpha_1 = b_1\delta_2$ é mmc de $\{b_1\alpha_1, b_2\alpha_1\} = \{\delta_1, \delta_2\}$. □

Observação 2.52. Logo, em domínios de Bézout duo, se δ for múltiplo comum a $\{\delta_1, \delta_2\}$, temos que ambos os fatores invariantes da matriz $\operatorname{diag}(\delta_1, \delta_2)$ dividem δ. Devido ao teorema 2.49, isto aplica-se a qualquer matriz quadrada diagonal. Isto é, se $\delta_1, \ldots, \delta_n$ dividirem δ, então todos os fatores invariantes da matriz $\operatorname{diag}(\delta_1, \ldots, \delta_n)$ dividem δ.

A observação anterior permite-nos concluir que o teorema 1.56 generaliza-se a DDEs comutativos, devido à sua demonstração original.

Notamos que a implicação (b) ⇒ (a) no teorema 1.57 generaliza-se a DDEs comutativos.

2.2.4 Fatores invariantes individuais da soma

A seguir, tal como na secção 1.3, consideramos os elementos na diagonal da forma normal de Smith, incluindo os zeros, como sendo os fatores invariantes.

Lema 2.53. *Seja R um DDE duo. Sejam $A, B \in M_{m,n}(R)$ cujos fatores invariantes são $(\alpha_i)_{i\in\mathbb{N}}$ e $(\beta_i)_{i\in\mathbb{N}}$ respetivamente. Seja $\gamma := \operatorname{mmc}(\operatorname{mdc}(\alpha_1, \beta_k), \ldots, \operatorname{mdc}(\alpha_k, \beta_1))$. Temos que γ divide um k-ésimo fator invariante de $A + B$.*

Demonstração. Segue diretamente do teorema 2.46. □

Teorema 2.54. *Seja R um DDE comutativo. Sejam $\alpha_1, \ldots, \alpha_q, \beta_1, \ldots, \beta_q \in R$ com $\alpha_i \mid \alpha_{i+1}$, $\beta_i \mid \beta_{i+1}$. Sejam $m \geq q$, $k \in \{1, \ldots, q\}$ com $k \neq m$. Seja $\gamma := \operatorname{mmc}(\operatorname{mdc}(\alpha_1, \beta_k), \ldots, \operatorname{mdc}(\alpha_k, \beta_1))$. Então existem $A, B \in M_{m,q}(R)$ (ou $A, B \in M_{q,m}(R)$), cujos fatores invariantes são $\alpha_1, \ldots, \alpha_q$ e $\beta_1, \ldots, \beta_q$ respetivamente, tais que γ é um k-ésimo fator invariante de $A + B$.*

Demonstração. A condição (a) do teorema 1.56 é satisfeita por γ. Logo obtemos (b), isto é, existem A, B de tamanhos adequados e com os fatores invariantes dados tais que pelo menos k fatores invariantes de $A + B$ dividem γ, ou seja, um k-ésimo fator invariante divide γ. Pelo lema anterior, obtemos que γ é um k-ésimo fator invariante de $A + B$. □

Isto é, $\operatorname{mmc}(\operatorname{mdc}(\alpha_1, \beta_k), \ldots, \operatorname{mdc}(\alpha_k, \beta_1))$ é o menor valor possível para o k-ésimo fator invariante de $A + B$.

Observação 2.55. Consideremos γ tal que $\operatorname{mdc}(\alpha_k, \gamma) = \operatorname{mdc}(\beta_k, \gamma) = 1$. A condição (a) do teorema 1.58 é satisfeita por γ^s para qualquer $s \in \mathbb{N}$. Logo obtemos (b), isto é, existem A, B de tamanhos adequados e com os fatores invariantes dados tais que pelo menos k fatores invariantes de $A + B$ são múltiplos de γ^s, ou seja, o $q - k + 1$-ésimo fator invariante é múltiplo de γ^s. Concluimos que, ou 0 é um possível $q - k + 1$-ésimo fator invariante de $A + B$ (o que, pelo corolário 1.59, acontece se e só se $\alpha_i \mid \beta_{i+q-k}$ e $\beta_i \mid \alpha_{i+q-k}$), ou o conjunto de possíveis valores do $q - k + 1$-ésimo fator invariante de $A + B$ não tem máximo.

Observação 2.56. Na maior parte dos anéis, existe sempre um γ nas condições anteriores. Um exemplo de um anel contraexemplo, é uma localização R_p. Aqui consideramos, por exemplo, $q = 3$, $\alpha_1 = p$, $\alpha_2 = \alpha_3 = p^2$, $\beta_1 = 1$, $\beta_2 = \beta_3 = p$. Tomamos $\gamma = p^s$ para algum $s \in \mathbb{N}$ ou $\gamma = 0$. Verifiquemos a condição (a) do teorema 1.58 para $k = 2$. Temos $\text{mdc}(\alpha_1, \gamma) = p \mid \beta_2$, $\text{mdc}(\beta_1, \gamma) = 1 \mid \alpha_2$, $\text{mdc}(\beta_2, \gamma) = p \mid \alpha_3$. Mas $\text{mdc}(\alpha_2, \gamma) = p^2 \not| \beta_3$ para $s \geq 2$ (assim como para $\gamma = 0$), pelo que os únicos possíveis valores para o segundo fator invariante de uma soma são 1 e p.

Considerações finais

O tema central da dissertação é o dos fatores invariantes do produto e da soma de matrizes. Introduzimos a noção de fatores invariantes em anéis não comutativos e com existência de divisores de zero, assim como introduzimos os conceitos de anéis duo e de anéis de Hermite. O estudo realizado conduziu-nos aos resultados apresentados neste capítulo. Permitiu-nos confirmar que a condição suficiente para anéis de Hermite e a condição necessária e suficiente para ADEs conhecidas aplicam-se também a anéis duo. Mostrámos que duas desigualdades relativas aos fatores invariantes soma e ao produto de matrizes respetivamente são válidas em ADEs duo. Consequentemente, pudemos fazer observações relativas aos possíveis valores de cada fator invariante individual da soma de matrizes. Demonstrámos como os anéis duo em que todas as matrizes diagonais têm a redução diagonal são exatamente os anéis de Bézout, como no caso comutativo. Como consequência destes resultados, também estendemos dois teoremas relativos aos fatores invariantes da soma ao caso duo.

No entanto, existem assuntos que não tivemos oportunidade de desenvolver na dissertação e que consideramos de interesse para trabalho futuro:

Um dos problemas de interesse a mencionar será o de determinar os possíveis fatores invariantes de uma soma de matrizes tendo em consideração a conjetura de Caldeira e Queiró. A determinação dos possíveis fatores invariantes de um produto de matrizes sobre um DDE é outra questão que fica em aberto, tendo como possibilidade mostrar que as desigualdades válidas conhecidas são suficientes para a existência das matrizes procuradas. O estudo, quer do problema da soma de matrizes como do problema do produto de matrizes, nos casos duo e com existência de divisores de zero, que iniciámos neste capítulo, é um assunto que consideramos poderá continuar a ser desenvolvido. Tendo como objetivo estudar os problemas mencionados acima, consideramos de interesse estudar os seguintes casos particulares:

- Generalizar o teorema 1.6 para ADEs duo, isto é, mostrar que, sendo $A, B \in M_n(R)$ não-singulares com fatores invariantes $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ respetivamente tal que $\text{mdc}(\alpha_i, \beta_j) = 1$ $\forall 1 \leq i, j \leq n$, e sendo $\gamma_1, \ldots, \gamma_n$ os fatores invariantes de AB, então $\gamma_i = \alpha_i\beta_i$. Tendo em conta o teorema 1.5 e o lema 2.30, só é necessário mostrar $\gamma_i \mid \alpha_i\beta_i$.

- Determinar os possíveis valores de cada fator invariante individual da soma de matrizes.

Bibliografia

[1] O. Azenhas, "The admissible interval for the invariant factors of a product of matrices", Linear and Multilinear Algebra, 46:1-2, 51-99

[2] O. Azenhas, E. M. de Sá, "Matrix realizations of Littlewood-Richardson sequences", 1990, Linear and Multilinear Algebra, 27:4, 229-242

[3] C. Caldeira, J. F. Queiró, "Invariant factors of products over elementary divisor domains", 2015, Linear Algebra and its Applications, 485: 345-358

[4] C. Caldeira, J. F. Queiró, "Sums of orbits of integral matrices", 2018, Linear and Multilinear Algebra, 66, 2421-2429

[5] D. Carlson, E. M. de Sá, "Generalized minimax and interlacing theorems", 1984, Linear and Multilinear Algebra, 15:1, 77-103

[6] M. G. Duffner, F. C. Silva, "On the interlacing inequalities for invariant factors", 2015, Linear Algebra and its Applications, 486, 443-448

[7] W. Fulton, "Eigenvalues, invariant factors, highest weights, and Schubert calculus", 2000, Bulletin of the American Mathematical Society, Vol. 37, Nº 3, 209-249

[8] L. J. Gerstein, "A local approach to matrix equivalence", 1977, Linear Algebra and its Applications, 16: 221-232

[9] O. Helmer, "The elementary divisor theorem for certain rings without chain condition", 1943, Bull. of the American Mathematical Society, Vol. 49, 225-236

[10] N. Jacobson, "The Theory of Rings", 1943, American Mathematical Society

[11] C. R. Johnson, "Precise intervals for specific eigenvalues of a product of a positive definite and a Hermitian matrix", 1989, Linear Algebra and its Applications, 117, 159-164

[12] I. Kaplansky, "Elementary divisors and modules", 1949, Trans. of American Mathematical Society, 66, 464-491

[13] T. Klein, "The multiplication of Schur-functions and extensions of p-modules", 1968, J. London Math Soc., 43, 280-284

[14] A. Klyachko, "Stable bundles, representation theory and Hermitian operators", 1998, Selecta Mathematica 4, 419-445

[15] T. Y. Lam, "A First Course in Noncommutative Rings", 2001, 2ª edição, Springer

[16] M. Larsen, W. Lewis, T. Shores, "Elementary divisor rings and finitely presented modules", 1974, Trans. American Math. Soc. 187, 231-248

[17] M. Newman, "On the Smith normal form", 1970, Journal of Research of the National Bureau of Standards - B. Mathematical Sciences, Vol. 75B, Nºs 1 e 2

[18] M. Newman, "The Smith normal form", 1997, Linear Algebra and its Applications, 254: 367-381

[19] J. F. Queiró, "Invariant factors as approximation numbers", Linear Algebra and its Applications, 1983, 49: 131-136

[20] J. F. Queiró, E. M. de Sá; "Singular values and invariant factors of matrix sums and products", 1995, Linear Algebra and its Applications, 225:43-56

[21] E. M. de Sá, "Hidden relations for the Smith invariants of a matriz sum", 1990, Portugal Math. 47, 417-422

[22] E. M. de Sá, "Imbedding conditions for λ-matrices", 1979, Linear Algebra and its Applications 24: 33-50

[23] E. M de Sá, "Interlacing problems for invariant factors", 1998, Textos Mat. Sér. B, Vol. 2, Universidade de Coimbra, Departamento de Matemática, Coimbra

[24] F. C. Silva, "On the invariant factors of the matrix XAY+B", 1987, Linear Algebra and its Applications, 96: 1-16

[25] F. C. Silva, "The rank of the difference of matrices with prescribed invariant factors", 1988, Linear and Multilinear Algebra, 24:1, 59-63

[26] H. J. S. Smith, "On systems of linear indeterminate equations and congruences", 1861, Philos. Trans. Royal Soc. London, 151: 293-326

[27] R. C. Thompson, "Interlacing inequalities for invariant factors", 1979, Linear Algebra and its Applications 24: 1-31

[28] R. C. Thompson, "Smith invariants of a product of integral matrices", 1985, em Linear Algebra and its role in Systems Theory, Contemporary Mathematics, 47: 401-435

[29] R. C. Thompson, "The Smith invariants of a matrix sum", 1980, Proceedings of the American Mathematical Society, Vol. 78, Nº 2

[30] R. C. Thompson, "Sums of integral matrices", 1986, Linear and Multilinear Algebra 19, 173-186